IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 2, Ver. VIII (Mar-Apr. 2014), PP 16-21
www.iosrjournals.org

Trust Modeling Scheme using Cluster Aggregation of Messages for Vehicular Ad hoc Networks

Vidhya. S[1], S.R. Mugunthan[2]
(Department of Computer Science and Engineering, SVS College of Engineering, Anna University, India)[1]
(Assistant Professor, Department of Computer Science and Engineering, SVS College of Engineering, Anna University, India)[2]

Abstract*: A VANET is a decentralized network as every node performs the functions of both host and router. The main benefit of VANET communication is the enhanced passenger safety by virtue of exchanging warning messages between vehicles. VANET differs from MANET as it provides higher mobility of nodes, larger scale networks, geographically constrained topology and frequent network fragmentation. This paper presents a detailed survey of trust management in VANETs. The paper consists of various ways for achieving trust in vehicular communications. Trust establishment is a major challenge in vehicular ad hoc networks as the outcome of the trust establishment process is a trusted relation between nodes. In critical applications like hazard warning a receiving node needs to ensure authenticity and trust-ability of received messages before reacting to them. Different trust establishment techniques exists each of them satisfies various properties such as scalability, privacy, intrusion detection, access control. Trust establishment may be decentralized, behavior-based, or certificate-based. Thus the aim of Trust management is to improve the security and reliability in VANET communications.*

Keywords*: VANET, Cluster-based, Trust, Confidence, direct and indirect- experience.*

I. Introduction

A Vehicular Ad hoc Network (VANET) is a special type of mobile ad hoc network (MANET) in which the nodes are vehicles that moves at high speed and uses short-range wireless communication. The VANET is used in many commercial applications like providing efficient routing information to the other vehicles, informing the drivers about the traffic conditions, accidents, road conditions etc. VANET uses various sensor devices, they are employed to observe the network conditions that helps for making a decision. Each sensor is capable of gathering relevant information and disseminates the data to other sensors. These low cost sensor devices are very small, and they can be deployed in a large numbers in the network without incurring high financial expenses.

VANET is an infrastructure-less network consisting of abundant mobile nodes and they communicate between themselves by a wireless medium on peer-to-peer basis. The nodes communicate with each other without the help of base-station. Secured information dissemination is a challenging task in these type of networks. Revealing confidential information to an un-intended receiver may damage the benefits that could be obtained from the VANETs.

Vehicular ad-hoc networks (VANETs) have a great potential to improve road safety, traffic congestions, fuel consumption, and to increase comfort level of passengers in vehicles. The goal of trust management in VANETs is to increase reliable delivery of information, to increase road safety and reduce traffic congestion by allowing information sharing among peers about road and traffic conditions. Trust management in VANETs help peers to detect false information provided by malicious/selfish nodes and take the appropriate driving decisions.

Standardizing is absolutely paramount task, for the evolution of VANET technology, and the current groups involved in this endeavor are Car-2-Car Communication Consortium (C2C-CC), Vehicle Safety Communications Consortium (VSCC), Continous Air Interface for Long and Medium Interface (CALM), Vehicle Infrastructure Integration Initiative, California PATH.

The objectives of deployment of VANET are to enhance the safety and efficiency of transportation systems. If the trust relationships are processed in real time, it is easy to take appropriate security measures and take correct decisions regarding any security issue. A trust based model can manage nodes dynamically and evaluate node's activities efficiently in a distributed manner. Illegitimate nodes can be detected based on their trust evaluations so that they cannot be used in any communication within the network. Thus computing trust values plays crucial role for improvement of the network security and reliability.

II. ISSUES IN Vanets

Establishing trustworthiness in VANETs impose several challenges. Firstly, the mobile nature of nodes. The nodes/vehicles in the network are roaming in the environment, which causes frequent link breaks and message loss. Due to high mobility the protocol cannot be handshake based and most of the communications are between nodes that have never interacted before therefore learning based scheme should be introduced so that they learn to know about each others behaviors.

Second, no centralized infrastructure present. The nodes may join or leave the network at any time. Thus it is decentralized in nature. There is no guarantee that the interaction will be with the same vehicle always. And in such an environment, it is not certain to decide whom to trust.

Third, trust establishment between the moving nodes must be achieved in real-time. As the major VANET applications are used for congestion avoidance, menace warning and warning informations in the case of accidents, so applications require strict time limit for message delivery.

Fourth, ability to tolerate with sparsity. For instance, at a particular time the road is completely exhausted, therefore the valuable information remain undelivered to peers. Solution is to increase the weight associated to the message, or to use role-based approaches (in which the trust associated with specific roles is pre-defined).

Fifth, various attacks on messages send is another important issue to be addressed for establishing trust in VANETs. Some common attacks are Sybil attack, newcomer attack, betrayal attack, inconsistency attack, bad mouthing attack and collusion attacks.

Sixth, increasing care about privacy. Identity preservation is another issue that has to be addressed and the proposed solution involves the use of pseudonyms or temporary identities that can be assigned by a centralized key distribution agency.

III. Vanet Applications

Major applications of VANET include providing safety information, traffic management and monitoring, and comfort related services, location based services and infotainment. Major applications of VANET include providing safety related information to avoid collisions, reducing accumulation of vehicles after an accident had occurred and offering cautionary related informations to status of road condition and intersections. Affixed with the safety related information are the liability related messages, which would determine which vehicles are present at the site of the accident and later help in fixing responsibility for the accident.

Road safety certainly is the main motivation of many researchers and represents the major issue in Intelligent Transportation Systems (ITS). Accidents are often caused by a faulty driver behavior, bad weather conditions or mechanical problems. One of the most important solutions to this problem relies on using vehicular communications to anticipate road accidents, extend road visibility and disseminate safety information. Traffic Management and Monitoring, they aim at improving traffic flow and road usage, providing timely information about the traffic state along many kilometers. The goal of comfort applications is to offer novel on board services to improve the travel experience, improving common multimedia capabilities of current commercial vehicles. Location-based Services is another effective service, which includes finding the nearest fuel station, ATMs, hotels etc. Although, GPS systems provides such kinds of services, it can also be realized using VANET.

Some important applications of VANETs are Life-critical safety, Safety warning, Electronic toll collection, Internet access, Automatic parking, Roadside service finder, Driver assistance, Weather conditions.

IV. VARIOUS TRUST MODELS FOR Vanets.

Merrihan et al,[1] A Categorized Trust- Based Message Reporting Scheme for VANETs (CTMR). This work presents a categorized decentralized trust management and evaluation scheme for nodes in VANETs. Role-based trust and experience-based trust is unified to form a combined trust scheme, and an opinion piggybacking process is used when needed. The nodes involved in interactions are evaluated individually during event reporting. A node is assigned a category level according to its trust value and a confidence measure that determine the degree of trustworthiness of a node's generated reports. The history of the driver's interactions with other vehicles is accounted.

CTMR[1] presents a node trust management framework for VANETs. This trust model is a categorized decentralized scheme. Proposed scheme introduces a penalty system to monitor malicious nodes and traces their actions through time. The model forms an advisory network for V2I and V2V communications, and efficient message verification for broadcasting purposes by RSU.

The CTMR considers only opinions from trusted nodes by the advisory network and discards reports generated from distrusted nodes by the message verification process. It guarantees to recipient nodes that

messages they received are reliable and trustworthy. It also prevents network congestion by disabling malicious nodes from logging into the network.

Riaz et al, [2] Intrusion-aware trust model for VANETs, a novel trust management scheme for identity anonymous vehicular ad hoc networks is proposed. The proposed method is robust and also it detects false location and time information. Furthermore, the analysis of the algorithm shows that it introduces linear time complexity, thus it is suitable to use in real time.

Their scheme works in three phases first for calculating confidence, based on the confidence value trust for each unique message is computed in second phase, this trust value is used for making a decision as to follow the message or not in third phase. The Intrusion-aware trust model analysis and evaluation shows that it achieves security resiliency and robustness in the presence of malicious node sending false information to misguide other nodes. Trust management scheme will not allow malicious nodes to increase the trust value of untrustworthy message. The trust value obtained in the non-malicious environment will always be greater than the trust value obtained in the malicious environment. Whenever a malicious user provides false values about source location and time of event, then the proposed method will return to 0 trust value.

The limitation of the Intrusion-aware trust model is that the location and time verification approaches work accurately, if the receiver receives the signal directly from the sender. If in between the transmitter and the receiver, any obstacle is present that causes reflection of the signal then it will increase the false positive rate.

Chen et al, [4] Trust modeling for message relay control and local action decision making in VANETs. The framework is used to support the effective evaluation of information sent by peers and the immediate control of false information in a VANET. It collects peer's trust opinions about a message sent by a peer during the propagation of the message.

The basic idea of framework is to evaluate and disseminate a message on the basis of its quality. Messages are evaluated in a distributed and collaborative fashion. In the trust-based approach the quality of a message is mapped to a trustworthiness value which can be computed from a collection of distributed feedbacks from other peers in the network.

To achieve scalable trust opinion aggregation, a cluster-based data routing mechanism. The system becomes more scalable due to clustering of peers, and message relay is performed between cluster leaders instead of between two neighboring peers. The majority opinion computed from trust opinions as the decision of the relay control model, which further increases the scalability of the network by reducing the network bandwidth utilized by malicious messages. Each peer's trust is evaluated by a trust metric: either a role-based trust or a experience-based trust. The framework evaluates scalability and effectiveness against malicious nodes presence and protects peers. Their trust model is binary (either fully trusted or not trusted). Inferring binary trust relationship is not always possible specially when the information is incomplete or when we are in uncertain situations. Furthermore, in their model, privacy and robustness is not extensively addressed.

F. G. Mármol and G. M. Pérez [6], TRIP, a trust and reputation infrastructure-based proposal for vehicular ad hoc networks. The main goal of TRIP is to identify malicious node quickly and accurately. Trust and reputation model is generally described as, each time a vehicle receives a traffic warning or a message from another, it first examines the reputation of the sender node in order to determine whether to reject and drop the message, to accept it but do not forward it, to accept and forward message. Nodes are classified and categorized within above three different trust levels represented with fuzzy sets for taking a decision.

In TRIP, the reputation of a node is first calculated on the basis of three factors: (1) direct previous experiences with the target node; (2) recommendations from other surrounding vehicles; and (3) recommendation from central authority through road side units. Then the system maps the reputation score with one of the three trust levels ((1) trust; (2) not trust; and (3) +/– trust), which are represented as fuzzy sets. If the reputation score of the targeting node belongs to a trust level, named 'not trust', then the message is discarded and notification about the presence of the malicious node is sent to the infrastructure. If the reputation score is 'trust', then node will accept that message and also forward it to the neighboring nodes. If the reputation score is '+/– trust', the message is accepted as reliable with a certain tunable probability, but it will not be forwarded to other neighboring nodes. The proposed scheme(TRIP) is based on the assumption, that a vehicle regularly circulates over the same road, and at the same time of the day. Thus an history is built. Privacy can be preserved by assigning pseudonyms to the vehicles.

Gurung et al, [3], Information-oriented Trustworthiness Evaluation in Vehicular Ad-hoc Networks. The proposed trust model directly evaluates the trustworthiness of the content of a message received from other vehicles. The model is built on factors such as content similarity, content conflict and route similarity.

A Real-time Message Content Validation (RMCV) scheme, which endows an individual vehicle with the capability of evaluating the trustworthiness of the possibly large amount of messages received in VANETs, without depending on road-side units or central servers. Thus infrastructure is minimum in this approach. RMCV consists of two main components: (i) Message Classification; and (ii) Information-oriented Trust Model. For message classification, a two-level clustering algorithm is used. First level of clustering, groups messages

describing the same event regardless the message content. A second level clustering is conducted on each cluster obtained from the first level clustering that aims to identify conflicting information regarding the same event.

Information-oriented trust model quantifies the impact of message trustworthiness and integrates their effects to generate an overall trustworthiness score that can be easily understood by end users for making decisions.

Experiments conducted on this scheme was feasible and efficient to meet the strict time constraint in real-time applications, the model was also highly tolerable when there are few conflicting information, and becomes more sensitive when the number of false reports increases enormously. Impact of False Messages on Vehicles Accepting True Messages was also experimented. To improve the accuracy, integrate in-depth message content analysis techniques.

Minhas et al, [10], A Multifaceted Approach to Modeling Agent Trust for Effective Communication in the Application of Mobile Ad Hoc Vehicular Networks. A multifaceted approach for modeling trust in VANET environments incorporates multiple faces of trust such as role-based, experience-based, priority-based, and majority-based trust and is able to restrict the number of reports that are received from other agents. The outcome of multi-faceted trust management is aggregated feedback for a certain request/event and an associated confidence value for it. The value of confidence depends on the reliability of estimated experience-based trust of each other agent and the maximum accept error rate for the aggregated feedback. For a fixed error rate, higher value of confidence(a value closer to 1), was resulted from considering more evidence or metrics having high reliability.

Experiments were conducted on various trust metrics. (1) Effect of Liars on Average Speed: Average speed of vehicles in the network decreases as the percentage of liars increases.(2) Effect of Liars on Average Speed: The overall average speed of the nodes increases, with an increase in the number of authorities in the environment, countering the effect of malicious agents. This shows the effectiveness of role-based trust in their model. (3) Countering Liars With Experience-Based Trust: the more experience an agent has with other agents, it can more effectively cope with the lying behavior of other agents. Experiments were done to study the effects of combining Role- and Experience-Based Trust and whether the model copes with sparsity.

The multi-faceted trust model is aimed to be decentralized, location/time specific, event/task specific, able to cope with the data sparsity problem, cumulative in order to be scalable, sensitive to privacy concerns, and able to support system-level security.

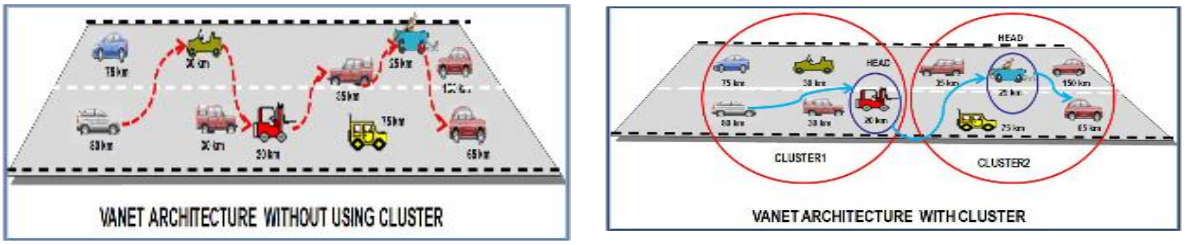
Sushmita Ruj et al, [8], On Data-centric Misbehavior Detection in VANETs. The problem of identifying false data is termed as data-centric misbehavior detection. The proposed work detects false alert messages and misbehaving nodes by observing their actions after sending out the alert messages. With the data-centric Misbehavior Detection Scheme (MDS), each node can decide whether an information received is true or false. The decision is based on the reliability of recent messages and new alerts with reported and estimated vehicle positions.

MDS reduces the communication and computation costs in calculating, transmitting, and storing certificate revocation lists. This approach does not rely on voting schemes and group associations. Thus it is immune to Sybil attacks. False location information can be detected in addition to detecting false alert messages. This scheme achieves adequate location privacy, by employing pseudonyms.

Huang et al, [7], Limitations of Trust Management Schemes in VANET and Countermeasures. This paper addresses the two main limitations: Information cascading and oversampling. One way to resolve this issue is to give weight to the decisions made by nodes. That is, nodes which observe an event are considered with weight 1. Less weight is given to nodes, which are at two or more hops from the direct observers. Majority voting for decision making results in a higher percentage of incorrect decisions in VANET. Considering only the opinions of nodes, which have directly observed the events have higher chance of correct decision making.

V. Proposed System

A trust opinion aggregation scheme is used in vehicular ad hoc networks, to support trust models used to evaluate the quality of information shared among peers in the environment. The topology of aggregation is based on a cluster-based message routing mechanism. For each cluster, a cluster leader is chosen randomly. Trust opinions are aggregated when the message from cluster is propagated through multiple hops. Thus each cluster receives an aggregated message from the previous hop clusters, and this message is passed on to the cluster members. Once the message is broad-casted cluster leader waits for the members opinion and forms new aggregated message, and it is relayed on to the next clusters.



Trust-based message evaluation allows each peer to evaluate the trustworthiness of the message by also taking into account other peers' trust opinions about the message and the peer-to-peer trust of these peers. This derives an effective local action decision for the peer. To implement message aggregation scheme an secure and efficient aggregation schemes is essential. One solution is to use signature along with each message being sent. By appending signature with the message, it cannot be maliciously modified without being detected. Once messages are signed peers cannot deny that the messages are sent by them. In order to achieve system scalability the aggregation scheme should be efficient.

The message relay control should be trust based, filtering out spam messages which utilizes the scarce resource such as channel bandwidth, to promote network scalability. Presence of malicious nodes is to be detected, and reduce their nodes weight in the network thus controlling the hazardous situations. Based on the parameters such as location of the message originator, and the freshness of the message, that is the time at which the message was generated as used to detect the malicious messages. It is worth to detect the trust on data-centric than on the entity-centric.

To improve the efficiency of the trust based aggregation scheme, it will be useful to incorporate following improvements, Due to complex road settings only a subset of trust opinions is available for aggregation, thus the effectiveness of the system should be measured in the absence of some of the trust opinions. Density of vehicles is another parameter for evaluating the aggregation mechanism. Since nodes in VANET have high mobility, thus at some instance number of nodes may be high or the there may be very less number of vehicles in road. The aggregation mechanism must have the capability to cope with the density of vehicles and with data sparsity.

Another suggestion is to examine the robustness of the aggregation mechanism, where the message aggregation may take long time. To evaluate the resistance of the system sophisticated attack models may be employed such as collusion attack, sybil attack. It is important to distinguish whether the report that is received is on the basis of direct or indirect evidence, in order to determine its potential trust value. The main idea is that an agent that asks for information from other agents will value advice from the direct witnesses more than that from the indirect ones. Detailed Data Flow Diagram is as follows:

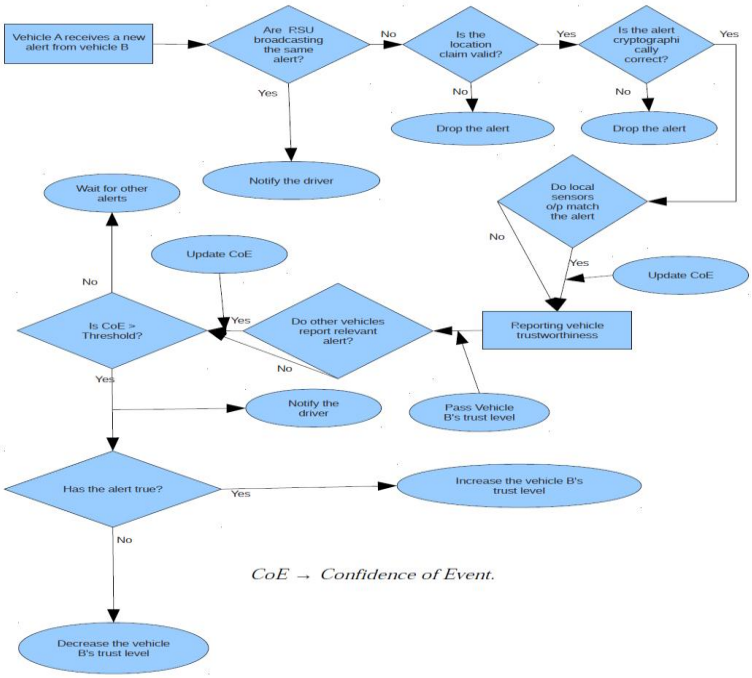


Fig: 1 DFD for Trust Calculation

In order to encourage honest reporting in VANET environment by introducing an penalty system. An agent B is considered dishonest by an agent A if the personal experience trust value that A has on B falls below some value that A can accept.

VI. Conclusion

This paper presents a detailed survey on various trust establishment techniques used in VANETs. This paper helps to think more in the direction of establishing more effective trust management schemes in VANETs. Deployment of trust management schemes helps to improve safety, life-critical and road conditions to reduce the number of car accidents and traffic congestion.

References

[1] Merrihan Monir, Ayman Abdel-Hamid, and Mohammed Abd El Aziz. "A Categorized Trust-Based Message Reporting Scheme for VANETs". Advances in Security of Information and Communication Networks in Computer and Information Science Vol 381, Springer Link(2013).

[2] Riaz Ahmed Shaikh, Ahmed Saeed Alzahrani. "Intrusion-aware trust model for vehicular ad hoc networks". Published in Wiley Online Library in Security and Communication Networks (Aug 2013).

[3] Sashi Gurung, Dan Lin, Anna Squicciarini, and Elisa Bertino, "Information-oriented Trustworthiness Evaluation in Vehicular Ad-hoc Networks". Published in the 7th International Conference on Network and System Security(2013).

[4] Jie Zhang, Chen Chen, Robin Cohen. "Trust modeling for message relay control and local action decision making in VANETs". Published in Security and Communication Networks,Volume 6(1)(2013).

[5] Jyoti Grover, M.S.Gaur, and V.Laxmi. "Trust Establishment Techniques in VANET". Published in Springer Link, Wireless Networks and Security Signals and Communication Technology (2013).

[6] Gómez Mármol F, Martínez Pérez G. "TRIP,a trust and reputation infrastructure-based proposal for vehicular ad hoc networks". Published in Elsevier, Journal Network Computer and Applications, Volume 35, Issue 3,(2012).

[7] Zhen Huang, Sushmita Ruj, Marcos Cavenaghi, Amiya Nayak. "Limitations of Trust Management Schemes in VANET and Countermeasures". In IEEE 22nd International Symposium on Personal, Indoor and Mobile Radio Communications,(2011).

[8] Sushmita Ruj, Marcos A. Cavenaghi, Zhen Huang, Amiya Nayak, and Ivan Stojmenovic. "On Data-centric Misbehavior Detection in VANETs". Published in:Vehicular Technology Conference (VTC Fall), 2011 IEEE, 5-8(2011).

[9] Umar Farooq Minhas, Jie Zhang, Thomas Tran, Robin Cohen. "Intelligent Agents in Mobile Vehicular Ad-Hoc Networks: Leveraging Trust Modeling Based on Direct Experience with Incentives for Honesty". Web Intelligence and Intelligent Agent Technology (WI-IAT), 2010 IEEE/WIC/ACM International Conference on (Volume:2), Aug. 31 2010-Sept. 3 2010.

[10] Minhas, U.F., Zhang, J., Tran, T., Cohen, R.: Intelligent Agents in Mobile Vehicular Adhoc Networks: Leveraging Trust Modeling Based on Direct Experience with Incentives for Honesty. In: Proceedings of the IEEE/WIC/ACM International Conference on Intelligent Agent Technology, Toronto, Canada, vol. 2, pp. 243–247 (2010)

[11] Zhang, J.: Trust Management for Vanets: Challenges,Desired Properties and Future Directions. International Journal of Distributed Systems and Technologies, 48–62 (2011)

[12] Huang, Z., Ruj, S., Cavenaghi, M., Nayak, N.: Limitations of Trust Management Schemes in VANET and Countermeasures. In: International Symposium on Personal, Indoor and Mobile Radio Communications, Toronto, Canada, pp. 1228–1232. IEEE (2011)

[13] Zhang, J.: A Survey on Trust Management for VANETs. In: International Conference on Advanced Information Networking and Applications, Biopolis, Singapore, pp. 105–112. IEEE (2011)

[14] Raya, M., Papadimitratos, P., Gligor, V.D., Hubaux, J.: On Data-Centric Trust Establishment in Ephemeral Ad Hoc Networks. In: The 27th Conference in Computer Communications, INFOCOM, USA, pp. 1238–1246. IEEE (2008)

[15] Golle, P., Greene, D., Staddon, J.: Detecting and Correcting Malicious Data in VANETs. In: Proceedings of the 1st ACM International Workshop on Vehicular Ad Hoc Networks, Philadelphia, PA, USA, pp. 29–37 (2004)

[16] Dotzer, F., Fischer, L., Magiera, P.: A Vehicle Ad-hoc Network Reputation System. In: Proceedings of the IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks, Giardini Naxos, Italy, pp. 454–456 (2005)