INTERNATIONAL JOURNAL OF
ADVANCE RESEARCH, IDEAS AND
INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume 5, Issue 5)
Available online at: www.ijariit.com

Resisting SBZ attack patterns by a reliable trust model in Vehicular Ad Hoc Network (VANET)

Selvarani B.
manipremi648@gmail.com

Rahin Batcha R.
batchabaksha@gmail.com

ABSTRACT

Vehicular ad hoc networks (VANETs) have the probable to convert the way people travel through the formation of a safe interoperable wireless communications network that contains buses, cars, traffic signals, cell phones, and other devices. However, VANETs are susceptible to security threats due to growing reliance on computing, communication, and control technologies. The sole security and privacy challenges modelled by VANETs include integrity, no repudiation, confidentiality, real-time operational constraints/demands, access control, privacy protection and availability. In this paper, we recommend that the new trust management scheme mainly focuses on the Traffic Estimation and Prediction System which generally provides the predictive information needed for proactive traffic control and traveller information. In VANETs singular vehicles can help each other's find assets and build up dependability under profoundly powerful conditions; without any unified trust expert to determine the precision and unwavering quality of data aggregated in a distributed manner we present a new trust management system for such networks. The trustworthiness of VANETs could be upgraded by addressing holistically both node trust, which is defined as how trustworthy the nodes in VANETs are and data trust, which is defined as the assessment of whether or not and to what extent the reported traffic data are trustworthy. To make this trust-based system robust we include a way of dealing with false ratings. More specifically a reliable trust model is proposed which can resist the SBZ attack patterns by using the cloud watch mechanism which can exclude potential lies. The effectiveness and efficiency of the proposed scheme are validated through extensive experiments. The proposed trust management theme is applicable to a wide range of VANET applications to improve traffic safety, mobility, and environmental protection with enhanced trustworthiness.

Keywords— *Vehicular Ad hoc Networks (VANETs), Security, Trust management, SBZ, Cloud watch mechanism*

1. INTRODUCTION

In recent years, the growing needs for increased safety and efficiency of road transportation system have promoted automobile manufacturers to integrate wireless communications and networking into vehicles. The wirelessly networked vehicles naturally form Vehicular Ad-hoc Networks (VANETs), in which vehicles cooperate to relay various data messages through multi-hop paths, without the need for centralized administration. VANETs have the potential to transform the way people travel through the creation of a safe, interoperable wireless communications network. In VANETs, various nodes, such as vehicles and Roadside Units (RSUs), are generally equipped with sensing, processing, and wireless communication capabilities. Both Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communications enable safety applications that provide warnings regarding road accidents, traffic conditions (e.g., congestion, emergency braking, icy road) and other relevant transportation events. However, VANETs are vulnerable to threats due to increasing reliance on communication, computing and control technologies. The unique security and privacy challenges posed by VANETs include integrity (data trust), confidentiality, no repudiation, access control, real-time operational constraints/demands, availability, and privacy protection. One typical application of VANETs is the Traffic Estimation and Prediction System (TrEPS), which generally provides the predictive information needed for proactive traffic control and traveller information. TrEPS will facilitate and enhance planning analysis, operational evaluation, and real-time advanced transportation systems operation. To help TrEPS more accurately evaluate the current traffic conditions and better make predictions, multiple emerging information sources have been taken into consideration, such as real-time location sensor data collected and transmitted by Android smartphones or Apple I Phone [7], community-based traffic and road condition reporting service based on crowdsensing [8], etc. All these emerging information sources need networking support, such as VANETs, to efficiently share and disseminate the collected traffic information.

However, sometimes the TrEPS may encounter confusing or even conflicting traffic information reported by multiple sources. Only a few trust models have recently been proposed for enforcing honest information sharing in vehicular networks. In this section, we summarize them and point out their issues.

Note that great efforts have been spent by researchers in security and privacy on trust establishment in VANETs that relies on security infrastructure and most often makes use of certificates. We focus on trust models that do not fully rely on the static infrastructure and thus can be more easily deployed. In these models, peers may form trust relationships with each other based on, for example, past interaction experience. They may also gather environmental information about messages sent by other peers to determine the correctness of the data. These models can be grouped into three categories, entity-oriented trust models, data-oriented trust models, and combined trust models. Entity-oriented trust models focus on the modelling of the trustworthiness of peers.

2. RELATED WORKS

Buchegger and J.-Y. Le Boudec Proposed a protocol, namely CONFIDANT (Cooperation of Nodes, equity in Dynamic advert-hoc Networks), to inspire the node cooperation and punish misbehaving nodes. CONFIDANT has 4 components in each node: a reveal, a popularity machine, a trusted supervisor, and a path supervisor. The reveal is used to study and identify ordinary routing behaviours. The recognition machine calculates the recognition for every node according to its observed behaviours accept as true with manager exchanges indicators with other accept as true with managers concerning node misbehaviours. The route manager continues course scores and well responses to diverse routing messages. A possible drawback of CONFIDANT is that an attacker may deliberately unfold fake signals to different nodes that a node is misbehaving at the same time as it's far definitely a well-behaved node. Consequently, it's far critical for a node in CONFIDANT to validate an alert it receives before it accepts the alert.

Incentive-based collaboration has been proposed in [3], [15]. Nuggets rely on a security module that uses tamper-proof hardware, whereas the Sprite system relies on a centralized Credit Clearing Service and a software protocol to ensure fair sharing of bandwidth. Michiardi and Molva [9] have proposed a game-theoretic approach to evaluate the cooperation enforcement mechanisms in mobile ad hoc networks. In their approach energy conservation (battery power) is considered to be the primary reason for node selfishness, and each node seeks to maximize a utility function. Nodes are assumed to be rational i.e. nodes will behave only in selfish interest but malicious behaviour for intangible benefits is not considered.

Srinivasan *et al.* [13] propose an analytical model on similar lines seeking an optimal operational point between cooperation and non-cooperation in relaying sessions for other devices. They too address the issue of optimized use of constrained energy resources to maximize device lifetimes. Their focuses are on providing an analytical model for attaining an optimal operation point for the MANET and assume that authentic information about most other nodes in the MANET, e.g. the energy class acceptance rates and other parameters involved in computing the utility function are available. Malicious behaviour is however discounted, i.e. nodes are considered to act only in selfish interest and not for intangible benefits. The computation of such an optimal operation point depends on the assumption that sufficient information about the system is available. They acknowledge the need for a distributed mechanism to reliably acquire and disseminate all such required information. However, normally only partial information is available, furthermore judging its accuracy is limited by the reputation information available for the device providing it. In realistic situations getting timely, accurate, and reliable information from unverifiable sources is difficult and remains a challenging problem. With lack of centralized systems to provide reliable data or provide security mechanisms. Reputation systems seek to maintain updated and correct reputations in a distributed manner based on observed behaviour and recommendations from others.

Several reputation systems have been proposed that are applicable in peer-to-peer and MANET environments e.g., [11], [7], [8] that provide trustworthiness metrics i.e. softer security guarantees when using second-hand information.

The analytical models like [13] and game-theoretic approaches like [9] provide insights on using reputations and incentives to promote cooperation and fair sharing. The focus of previous approaches has been on session-based interactions, whereas the data interactions in our scenarios are predominantly based on those triggered by epidemic updates. In our scenario, ad hoc connectivity merely provides connectivity to the source once an information source has been discovered. We seek to promote collaborative behaviour at the application level, over and above regulation, i.e. beyond mere conformance to the communication protocol specifications. Such collaborative mechanisms are necessary and justified when it is possible to identify a set of identities that reciprocate. To be able to identify such a workable set of identities we use local landmarks and context markers and use cooperation scores as incentives to reciprocate. We assume that the battery power is no longer a problem, e.g. devices like cars where battery power is not a limitation. However the reliability, availability and quality of the data provided and the cooperation/collaboration offered by other devices in finding information is more important.

3. TRUST MODELS IN VANET

3.1 Entity-oriented Trust Model

Two typical entity-oriented trust models are the sociological trust model proposed by Gerlach and the multi-faceted trust management model proposed by Minhas et al. The sociological trust model is proposed based on the principle of trust and confidence tagging.

Gerlach has identified various forms of trust including situational trust – which depends on the situation only; dispositional trust which is the level of trust based on a peer's own beliefs, system trust depends on the system and finally belief formation process – which is the evaluation of data based on previous factors. Additionally, they have presented architecture for securing vehicular communication and a model for preserving location privacy of the vehicle. However, Gerlach does not provide formalization of the architecture about how to combine the different types of trust together. The multi-faceted trust management model of Minhas et al. Features in the role-based trust and experience-based trust as the evaluation metric for the integrated trustworthiness of vehicular entities. This model also allows a vehicular entity to actively inquire about an event by sending requests to other entities but restrict the number of reports that are received. For this purpose, the authors introduce in the research the concept of priority-based trust, which provides for an ordering of the value of an information source within a role category, using the influence of experience-based trust. The limit on the number of sources consulted is sensitive to the task at hand. In the end, the trust of information sources and the contextual information about the event such as time and location are integrated into a procedure for gauging whether majority consensus has been reached, which ultimately determines the advice a vehicular entity should follow. The above two trust models have some components in common, for example, situational trust can be compared with event/task-specific trust, and similarly dispositional trust can be compared to experience or role-based trust. One problem about the multi-faceted trust management is that robustness has not been extensively addressed.

3.2 Data-Oriented Trust Model

In contrast to the traditional view of entity-oriented trust, Raya et al. propose that data-oriented trust may be more appropriate in the domain of Ephemeral Ad-hoc Networks such as VANETs. Data-centric trust establishment deals with evaluating the trustworthiness of the data reported by other entities rather than the trust of the entities themselves.

In their model, they define various trust metrics of which a priori trust relationships in entities is just one of the default parameters and depends on the attributes associated with a particular type of node. Using Bayesian inference and Dempster-Shafer Theory, they evaluate various evidence regarding a particular event taking into account different trust metrics applicable in the context of a particular vehicular application.

Finally, their decision logic outputs the level of trust that can be placed in the evaluated evidence indicating whether the event related to the data has taken place or not. Raya et al. also propose the use of task/event specific trust metrics as well as time and location closeness. One of the shortcomings of their work is that trust relationships in entities can never be formed, only ephemeral trust in data is established, and because this is based on a per event basis, it needs to be established again and again for every event. This will work so long as there is enough evidence either in support of or against a specific event, but in the case of data sparsity their model would not perform well. Golle et al. present a technique that aims to address the problem of detecting and correcting malicious data in VANETs. The key assumption of their approach is in maintaining a model of VANET at every node. This model contains all the knowledge that a particular node has about the VANET. Incoming information can then be evaluated against the peer's model of VANET. If all the data received agrees with the model with a high probability then the peer accepts the validity of the data.

However, in the case of receiving data which is inconsistent with the model, the peer relies on a heuristic that tries to restore consistency by finding the simplest explanation possible and also ranks various explanations. The data that is consistent with the highest-ranking explanation(s) is then accepted by the node. The major strength of this approach is that it may provide security against adversaries that might even be highly trusted members in the network or might be colluding together to spread malicious data. However, one strong assumption of this approach is that each vehicle has the global knowledge of the network and solely evaluates the validity of data, which may not be feasible in practice.

3.3 Combined Trust Model

Three combined trust models have been proposed to model the trustworthiness of peers and use the modelling results to evaluate the reliability of data. Dotzer et al. have suggested building a distributed reputation model that exploits a notion called opinion piggybacking where each forwarding peer (of the message regarding an event) appends its own opinion about the trustworthiness of the data. They provide an algorithm that allows a peer to generate an opinion about the data based on aggregated opinions appended to the message and various other trust metrics including direct trust, indirect trust, and sender-based reputation level and Geo-Situation oriented reputation level. This last trust metric allows their model to introduce some amount of dynamism in the calculation of trust by considering the relative location of the information reporting node and the receiving node. Additionally, the situation-oriented reputation level allows a node to consider certain situational factors e.g. familiarity with the area, rural or metropolitan area etc. again introducing some dynamism in trust evaluation based on context. One problem is that the authors did not provide sufficient and complete details about the approach. Although they mention that sender-based reputation information is managed, they did not describe its formalization or how reputation information can be updated.

A more important problem about this approach is that it repeatedly makes use of the opinions from different nodes. The nodes that provide opinions about a message earlier will have a larger influence than the nodes generated opinions later because the earlier nodes' opinions will be repeatedly and recursively considered by later nodes. Patwardhan et al. propose an approach in which the reputation of a node is determined by data validation. In this approach, a few nodes, which are named as anchor nodes here, are assumed to be pre-authenticated, and thus the data they provide are regarded as trustworthy. Data can be validated by either agreement among peers or direct communication with an anchor node. Malicious nodes can be identified if the data they present is invalidated by the validation algorithm. One problem about this scheme is that it does not make use of reputation of peers when determining the majority consensus. The majority consensus works well only when a sufficient number of reports about the same event are provided. However, this scheme only passively waits for reports from other peers. Overcoming some problems of the above two models, Chen et al. propose a trust-based message propagation and evaluation framework in vehicular ad-hoc networks where peers share information regarding road condition or safety and others provide opinions about whether the information can be trusted.

More specifically, the trust-based message propagation model collects and propagates peers' opinions in an efficient, secure and scalable way by dynamically controlling information dissemination. The trust-based message evaluation model allows peers to evaluate the information in a distributed and collaborative fashion by taking into account others' opinions. This model is demonstrated to promote network scalability and system effectiveness in information evaluation under the pervasive presence of false information, which are the two essentially important factors for the popularization of VANETs.

4. PROPOSED WORK

The trustworthiness of VANETs could be upgraded by addressing holistically both node trust, which is defined as how trustworthy the nodes in VANETs are and data trust, which is defined as the assessment of whether or not and to what extent the reported traffic data are trustworthy. To make this trust-based system robust we include a way of dealing with false ratings. More specifically a reliable trust model is proposed which can resist the SBZ attack patterns by using the cloud watch mechanism which can exclude potential lies. The proposed trust management theme is applicable to a wide range of VANET applications to improve traffic safety, mobility, and environmental protection with enhanced trustworthiness. The flow diagram of the proposed trust model is illustrated in figure 1.

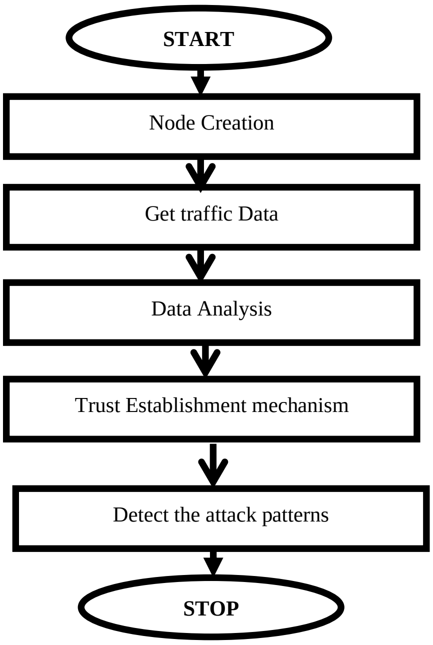

Fig. 1: Flow diagram of proposed reliable trust model

4.1 Data Trust

In the proposed reliable scheme, we first collect traffic data from VANETs for data analysis. Second, we summarize the findings from the data analysis as evidence for trust management schemes to evaluate the trustworthiness. Then this evidence will be used to assess the trustworthiness of data and nodes. The trustworthiness of nodes further consists of functional trust and recommendation trust. The details of the evaluation of trust recommendation using collaborative filtering are provided. View combination is very important for the proposed scheme. Because some of the traffic data are not reliable, it is critical to find a view 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 evidence so that both data trust and functional trust can be properly evaluated. In this work, Dempster–Shafer theory of evidence (DST) is used to fuse together multiple pieces of evidences even if some of them might not be accurate. In DST, probability is replaced by an uncertainty interval bounded by belief (*bel*) and plausibility (*pls*). Belief is the lower bound of this interval and represents supporting evidence. Plausibility is the upper bound of the interval and represents non-refuting evidence.

For instance, if a node N_A observes that one of its neighbours, say node N_B, has dropped packets with probability p, then node N_A has p degree of belief in the packet dropping behaviour of node N_B and 0 degrees of belief in its absence. More specifically, we use the Dempster's rule to combine the local evidence collected by a mobile node itself and the external evidence shared by other mobile nodes. The DST based view combination algorithm is shown in Algorithm1. Note that *nk* stands for the *k*-th node in VANET. *Vk* denotes the initial evidence that is collected by *nk*, and *V k* denotes the updated evidence that is possessed by *nk*.

4.2 Node Trust

The node trust indicates how trustworthy the nodes in VANETs are. The trustworthiness of vehicle nodes is assessed in two dimensions. In other words, a vector that is composed of two elements is used to describe the trustworthiness of each node. The two dimensions of node trust are functional trust and recommendation trust, which indicates how likely a node, can fulfil its functionality and how trustworthy the recommendations from a node for other nodes will be, respectively. It is well understood that it is not always feasible for two-vehicle nodes to communicate directly with each other in VANETs. In this case, it is essential for one vehicle node to relay data for others. However, sometimes a node may refuse to relay data either because of its limited battery power or other resources, or the node may have been compromised by adversaries. Therefore, it is critical to know whether or not another vehicle is trustworthy to interact with. If a vehicle has never interacted with others before, then the trust recommendations that it receives from others become the only data that it can rely on to evaluate the trustworthiness of other nodes. More specifically, the trust ratings of every node are viewed as a vector in the *k* dimensional space. If a node does not evaluate a node, then the default rating is used. The similarity between two nodes is measured by computing the cosine of the angle between these two vectors. Nodes which have similar trust preferences on some nodes may also have similar preferences on others. Thus, this method provides recommendations or predictions to the target node based on the opinions of other like-minded nodes.

For instance, if a node A wants to relay through a vehicle B, but it did not interact with it previously means, the only way to relay through B is based on the decision made by evaluating the trustworthiness of the node B. Node A collects the trust ratings from all the neighbours of B. Based on the trust rating the node A will decide whether to relay through the vehicle B. There is possible that some malicious nodes will send fake opinion and gives a false rating to A. such fake opinion spreaders are recognized as SBZ- Simple, Badmouth and Zigzag attack patterns. The proposed work will help to exclude the potential lies and detect these attack patterns.

4.3 Resisting SBZ Attack Patterns

The main goals of the malicious node may include intercepting the normal data transmission, forging or modifying data, framing the benign devices by deliberately submitting fake recommendations, etc. Cloud Watch Mechanism which is a traditional localization approach is used to detect the nodes which spread the fake recommendations to other nodes. This mechanism is based on averaged RSS from each node identity inputs to estimate the position of a node. However, in wireless spoofing attacks, the RSS stream of a node identity may be mixed with RSS readings of both the original node as well as spoofing nodes from different physical locations. Hence it can also identify the fake information in the network. When a node A is identified that it has spread a fake opinion about another node B in the network during node trust, the cloud watch mechanism will analyse that particular node's behaviour. It checks its packet delivery ratio and delay of the accused node A. If it finds that node A did not interact with node B previously, then it is identified as malicious. Else if A has low packet delivery ratio and high delay when interacted with B previously means it is not recognized as malicious. More specifically, the following malicious attacks pattern which spreads fake recommendations is considered in this paper.

Simple Attack (SA): An attacker may manipulate the compromised nodes not to follow normal network protocols 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. The simple attack patterns will misbehave with a probability of 0.5 and honestly shares the trust opinion with each other.

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 accurate trust evaluation and make it harder to successfully identify malicious attackers. The badmouth attack patterns misbehave with a probability of 0.5 and shares opposite trust opinion with a probability of 0.5.

Zigzag (On-and-off) Attack (ZA): Sometimes sly attackers can alter their malicious behaviour patterns so that it is even harder for the trust management scheme to detect them. For instance, they can conduct malicious behaviours for some time and then stop for a while (in that case the malicious behaviours are conducted in an on-and-off manner). In addition, the sly attackers can also exhibit different behaviours to different audiences, which can lead to inconsistent trust opinions to the same node among different audiences. Due to the insufficient evidence to accuse the malicious attacker, it is generally more difficult to identify such sly attackers. The zigzag attack patterns misbehave with a probability of 0.5 and honestly shares trust opinion with half of nodes and shares opposite trust opinion with another half of the nodes with a probability of 0.5

5. SIMULATION RESULTS

In this section, the performance of the proposed scheme is evaluated and the experimental results are presented. We use Network Simulator NS2 as the simulation platform, and Table I lists the parameters used in the simulation scenarios.

Table 1: Parameters used

Parameter	Value
Number of nodes	30
Transmission range	300m
Node placement	Random
Node motion speed	50m/s
MAC protocol	802.11

To evaluate how accurate the proposed scheme is when it is used to identify untrustworthy nodes in VANETs. Precision and recall values are calculated to determine the accuracy of the proposed trust model.

These two parameters are defined as follows.

Precision = (No. of. truly malicious nodes gathered)/ (Total number of untrustworthy nodes gathered)

Recall = (No. of. truly malicious nodes gathered)/ (Total number of the truly malicious node)

The simulation results show that the proposed trust model yields high performance in terms of precision, recall and low communication overhead even though when the vehicle moves faster.

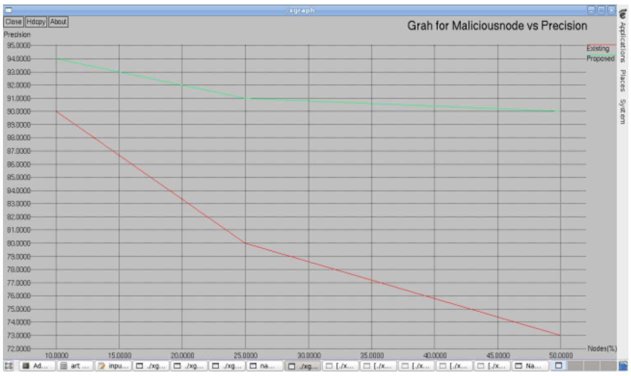

Fig. 2: Graph for Malicious Node vs. Precision

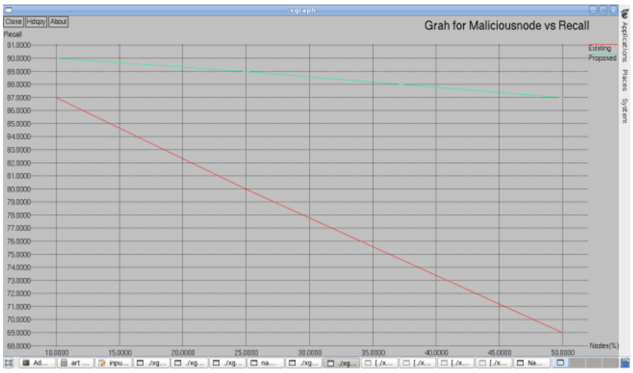

Fig. 3: Graph for Malicious Node Vs Recall

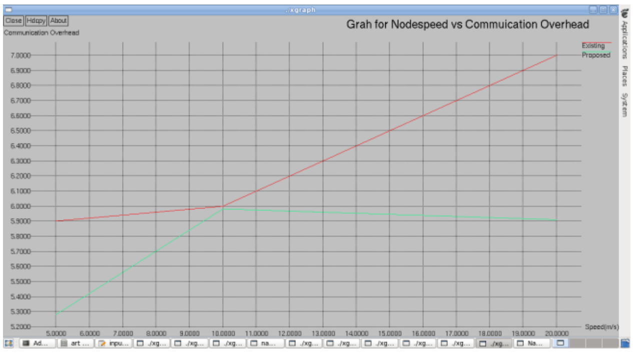

Fig. 4: Graph for Node Speed Vs Communication Overhead

6. CONCLUSION

In this paper, we recommend that the new trust management scheme mainly focuses on the Traffic Estimation and Prediction System which generally provides the predictive information needed for proactive traffic control and traveller information. It will facilitate and enhance planning analysis, operational evaluation, and real-time advanced transportation systems operation and it can provides input to traffic managers who decide where and when to post specific messages on variable message signs In vehicular ad hoc network individual vehicles can help each other's locate resources and establish trustworthiness under highly dynamic conditions, lacking any centralized trust authority to ascertain the accuracy and reliability of data aggregated in a distributed manner we present a new trust management system for such networks. To make this trust-based system robust we include a way of dealing with false ratings. Cloud watch mechanism is used to detect and exclude potential lies. More specifically three attack patterns are considered in the proposed system. The simulation results show the effectiveness and efficiency of the proposed scheme which is validated through extensive experiments.

7. REFERENCES

[1] J Yin, T ElBatt, G Yeung, B Ryu, S Habermas, H Krishnan, T Talty, in Proceedings of the 1st ACM International Workshop on Vehicular Ad Hoc Networks. Performance evaluation of safety applications over DSRC vehicular ad hoc networks (ACM, 2004), pp. 1–9.

[2] G Yan, S Olariu, MC Weigle, Providing VANET security through active position detection. Compute. Commun. 31(12), 2883–2897 (2008).

[3] Y-C Wei, Y-M Chen, in Information Security Applications, 13th International Workshop. Efficient self-organized trust management in location privacy-enhanced VANETs (Springer, 2012), pp. 328–344.

[4] Q Li, A Malip, KM Martin, S-L Ng, J Zhang, A reputation-based announcement scheme for VANETs.

IEEE Trans. Vehicular Technol. 61(9), 4095–4108 (2012).

[5] F Dotzer, L Fischer, P Magiera, in Sixth IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks. VARS: a vehicle ad-hoc network reputation system (IEEE, 2005), pp. 454–456.

[6] M Raya, J-P Hubaux, Securing vehicular ad hoc networks. J. Compute. Secure. 15(1), 39–68 (2007).

[7] S Gurung, D Lin, a Squicciarini, E Bertino, in Network and System Security. Information-oriented trustworthiness evaluation in vehicular ad-hoc networks (Springer, 2013), pp. 94–108.

[8] J.Zhang, 2012, ―Trust management for VANETs: challenges, desired properties and future directions. In International Journal of Distributed Systems and Technologies, pp.48-62.

[9] J.Zhang, 2011, ―A survey on trust management for VANETs in International Conference on Advanced Information Networking and Applications, pp.105-112.

[10] Z. Huang, S.Ruj, M.Cavenaghi, and A.Nayak, 2011, ―Limitations of trust management schemes in VANET and countermeasures‖ In IEEE 22nd International Symposium on Personal, Indoor and Mobile Radio Communications, pp.1228–1232.

[11] U.F.Minhas, J.Zhang, T.Tran, and R, Cohen, 2010,―Towardsexpanded trust management for agents in vehicular ad-hoc networks, In International Journal of Computational Intelligence: Theory and Practice (IJCITP), vol. 5, no.1.

[12] Gerlach, 2007, ―Trust for vehicular applications, International Symposium on Autonomous Decentralized Systems, pp.295-304.

[13] M.Raya, P.Papadimitratos, V.D.Gligor, J.Hubaux, 2008,―On Data-Centric Trust Establishment in Ephemeral Ad Hoc Networks, The 27th Conference in Computer Communications, IEEE, pp.1238-1246.

[14] C.Chen, J.Zhang, R.Cohen, and P.Han Ho, 2010, ―A trust-based message propagation and evaluation framework in VANETs, In Proceedings of the International Conference on Information Technology Convergence and Services.

[15] S.Ma, and J.Lin ―A survey on trust management for intelligent Transportation system In Proceedings of the 4th ACMSIGSPATIAL International Workshop on Computational Transportation Science IWCTS'11, pp.18-23, 2011.

[16] C. Leckie and R. Kotagiri, "Policies for sharing distributed probabilistic beliefs," in Proceedings of ACSC, 2003, pp. 285–290.

[17] S. Buchegger and J.-Y. Le Boudec, "Performance analysis of the confidant protocol," in Proc. 3rd ACM Int.Symp. Mobi Hoc Network. Compute. 2002, pp. 226–236.

[18] P. Michiardi and R. Molva, "CORE: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks," in Proc. IFIP TC6/TC11 6th Joint Working Conf. Commune. Multimedia Security, 2002, pp. 107–121.

[19] Patwardhan, A. Joshi, T. Finin, and Y. Yesha, "A data-intensive reputation management scheme for vehicular ad hoc networks," in Proc. 3rd Annul. Int. Conf. Mobiquitous Syst. Workshops, Jul. 2006, pp. 1–8.

[20] P. Golle, D. Greene, and J. Staddon, "Detecting and correcting malicious data in VANETs," in Proceedings of VANET, 2004.

[21] W. Li, A. Joshi, and T. Finin, "Coping with node misbehaviours in ad hoc networks: A multi-dimensional trust management approach," in Proc. 11th Int. Conf. MDM, May 2010, pp. 112–121.

[22] S. Buchegger and J.-Y. L. Boudec, "A robust reputation system for mobile ad-hoc networks," in Proc. P2PEcon, 2003, pp. 1–6.

[23] C. Chen, J. Zhang, R. Cohen, and P.-H. Ho, "A trust-based message propagation and evaluation framework in VANETs," Int. Conf. on Information Technology Convergence and Services, 2010.

[24] Rahman, S.U. and Hengartner, U., 2007, ―Secure crash reporting in vehicular Ad hoc networks‖. Proc. 3rd Intl. Conf. On security and Privacy in Communications Networks. IEEE Computer Society, pp.443-452.

[25] U.F.Minhas, J.Zhang, T.Tran, and R, Cohen, 2010,―Intelligent agents in mobile vehicular ad-hoc networks: Leveraging trust modelling based on direct experience with incentives for honesty. In Proceedings of the IEEE/WIC/ACM International Conference on Intelligent Agent Technology (IAT).

[26] M.Chuang and J.Lee, 2011,―TEAM: Trust extended authentication mechanism for vehicular ad hoc

[27] networks, Consumer Electronics, Communications and Networks (CECNet), IEEE International Conference, pp.1758-1761.

[28] I.Ahmed Sumra, H.Hasbullah, I.Ahmad, and J.Bin Ab Manan, 2011, Forming vehicular web of trust in VANET, Electronics, Communications and Photonics Conference (SIECPC), IEEE.

[29] S.Biswas, J.Misic, and V.Misisc, 2011, ID-based safety message authentication for security and trust International Conference on Distributed Computing Systems Workshops, IEEE, pp.323-331.

[30] I. Ahmed, H.Hasbullah, J.Lail, and M.Rehman, 2011, ―Trust and trusted computing in VANET", In Computer Science Journal, vol.1, issue1.