On the Design, Development and Implementation of Trust Evaluation Mechanism in Vehicular Networks

Farhan Ahmad*, Asma Adnane†, Chaker A. Kerrache‡, Fatih Kurugollu*, and Iain Phillips†
*Cyber Security Research Group, College of Engineering and Technology, University of Derby, Derby, United Kingdom
†Department of Computer Science, Loughborough University, Loughborough, United Kingdom
‡Department of Maths and Computer Science, University of Ghardaia, Ghardaia, Algeria
Email: *{f.ahmad, f.kurugollu}@derby.ac.uk †{a.adnane, i.w.phillips}@lboro.ac.uk ‡ch.kerrache@univ-ghardaia.dz

***Abstract*—**
Vehicular Ad-hoc NETworks (VANET) have revolutionised the intelligent transportation systems. Indeed, they enable vehicles to communicate with each other and with the infrastructure, and they facilitate several vital applications in real-time. Several trust models have been proposed to ensure a secured VANET and the authenticity, integrity and reliability of information exchanged in the network. The concept of trust models is to introduce and implement trust explicitly in the vehicular nodes. In this paper, we propose a lightweight evaluation methodology to evaluate trust models, specifically designed for VANET. Our study focused on the three categories of VANET trust models (TMs): Entity-oriented Trust Models (ETM), Data oriented Trust Models (DTM) and Combined Trust Models (CTM). Our simulations evaluate the efficiency of the trust models and compare them against several trust related parameters: false positive rate, precision and accuracy level in detecting malicious nodes. Since the scope of this research work is to evaluate the performance of TMs under adversary conditions, we have considered on-off attacks which can act as man-in-the-middle to drop and delay transmitted packets.

***Keywords*—Trust Models, Vehicular ad hoc networks, Internet-of-Things, Smart Cities, Intelligent Transportation Systems**

I. Introduction

The Internet-of-Things (IoT) has evolved rapidly over the past few years enabling every device with computation, storage and communication capabilities to connect to the Internet and provide a variety of applications including smart health, smart transportation, smart grids etc [1], [2]. The Vehicular Ad-hoc NETwork (VANET) is an important application of IoT, where smart and connected vehicles equipped with sensors (e.g., GPS, distance sensors, cameras etc.) communicate with each other to ensure traffic safety and improve traffic efficiency. This involves propagating sensitive information securely through the network. As a result, this information must arrive at the destination vehicles unchanged. However, VANET are large-scale networks which could contain misbehaving vehicles (or attackers) that have the ability to launch a wide range of attacks which can affect critical applications. These attacks include man-in-the-middle, Sybil, black-hole or denial-of-service in the network [3]–[6]. Providing and maintaining security within a VANET is extremely challenging.

In order to ensure security in VANETs, various solutions have been proposed that rely on traditional cryptography and a Public Key Infrastructure (PKI). However, a VANET is a very volatile network and as a result, the presence of such an infrastructure cannot be guaranteed. Furthermore, these solutions fail to identify insider attacks with valid certificates. In order to solve these issues, recently trust management is proposed as an alternative security measure, which has the ability to overcome the challenges posed by cryptographic-based solutions. Trust-based systems create a trusted environment where the vehicles can disseminate and share messages in collaboration. We define trust in VANET as *the assurance and faith which source vehicle places on the destination vehicle for the accomplishment of desired task*. However, evaluating trust in VANET is extremely challenging due to high mobility and random placement of the vehicles in the network. To date, various VANET trust models (TMs) are proposed with the aim to achieve security via trust management, for instance [7]–[10]. Every designed TM has different philosophy to compute trust. For instance, some other TMs compute trust based on the data transmitted and some TMs relies on sender's behaviour to calculate trust.

Current proposed TMs can be broadly categorized into three classes, namely: (1) Entity-based trust models (ETM), (2) Data-based trust models (DTM), and (3) Combined trust models (CTM) [11]–[14]. ETM computes trust on the vehicle itself to eliminate misbehaving vehicles from the network. DTM, on the other hand, establishes trust on the vehicles based on the received messages, while CTM combines the characteristics of both ETM and DTM for trust computation where both data and node trustworthiness is taken into account [15]. Under the umbrella of these TMs categories, vehicles can adapt any mechanism to establish trust in a VANET. Therefore, there should be a mechanism which can validate and evaluate these TMs in VANETs before integrating them within the real environment due to the sensitive nature involved. We propose a novel mechanism to evaluate and validate TMs in VANET. The major contributions of this paper are: (1) First, we propose a light-weight and efficient methodology to evaluate TMs in VANETs and (2) we validate our proposal using extensive simulations and compared the efficiency of three TMs from different categories.

The rest of the paper is organized as follows: Section II provide details about the proposed methodology and mechanism. Section III introduces the implemented TMs, followed by their performance evaluation in Section IV where the simulation setup and evaluation metrics are identified. Simulation results are presented and explained in Section V. The paper culminates with conclusions and future work in Section VI.

II. Proposed Methodology

In this section, we provide the details of our proposed mechanism that is designed for evaluating and comparing TMs. The high-level view of the proposed methodology is depicted in Fig. 1. This shows that our model has the following modules:

- Attacker Model
- Trust Models
- Initial Message Evaluation
- Data-Centric Trust Computation
- Node-Centric Trust Computation
- Overall Trust Evaluation

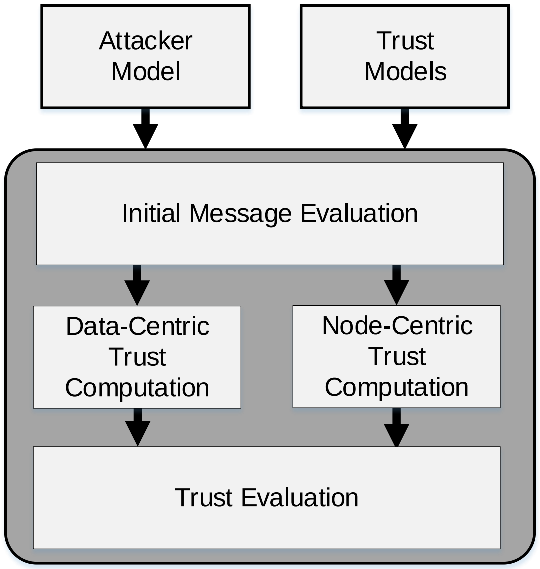
Attacker Model
Trust Models
Initial Message Evaluation
Data-Centric Trust Computation
Node-Centric Trust Computation
Trust Evaluation

Fig. 1. Proposed Methodology

A. Attacker Model

TMs ensure the propagation of trusted content within the network. This module is identified, so that the efficiency of the TM can be evaluated in presence of adversary nodes as they attempt to compromise the performance of the network. As a VANET is an open, decentralised and large-scale network, it faces a wide range of attacks including man-in-the-middle, on-off (zig-zag), denial-of-service, spoofing, bad-mouthing, black-hole and grey-hole attacks etc [3]–[6]. Therefore, this module is designed specifically for evaluating TMs in presence of attacker nodes. This module can contain any attack model. However, for this specific study, we considered on-off attack where the attacker is acting as a man-in-the-middle to drop or delay the data packets.

B. Trust Models

The next phase of our proposal is the identification of TMs in VANETs. In this phase, we identify TMs with different philosophy to evaluate trust in a VANET, i.e. the TMs can either establish and evaluate trust on data or entity or combined. In this paper, we identify three TMs (ETM, DTM, CTM) for the evaluation and comparison purpose, which evaluate trust using different techniques.

C. Initial Message Evaluation

In VANETs, every vehicle broadcasts messages which contains important information including data, location, time, and message IDs [16]. In this module, we performed an initial evaluation on the messages received from the vehicles based on two parameters: (1) Location approximation of node A ($AppLoc_A$), and (2) Message delivery time ($Time_{delivered}(M)$) of the message M. Every vehicle is equipped with GPS and map modules which are constantly updating throughout their journey in the network. This can be helpful to approximate the location of the message sender which can provide message coordinates in terms of X, Y and Z, i.e., $Coord(A)_X$, $Coord(A)_Y$ and $Coord(A)_Z$. A message is accepted only by the evaluator node (E_VN) if the coordinates of the message sender are present in the current map (V_M) of the vehicle, i.e., $Coord(A)_X, Coord(A)_Y, Coord(A)_Z \in V_M$.

On the other hand, when a message M is shared at the time $Time_{created}$, E_VN accepts the received message only if:

$$Time_{delivered} - Time_{created} \leqslant Threshold_{app} \tag{1}$$

In Equation 1, "$Time_{delivered}$" is the current time at the E_VN and "$Threshold_{app}$" represents the acceptable time threshold which depends on the severity of the application app used in VANET. For safety applications, $Threshold_{app}$ is usually set to 100 msec [17].

E_VN categorizes the messages as malicious if the sender vehicle fails to satisfy Equation 1 and the criteria that the message is received from the location, unknown to the E_VN. Messages satisfying these equations are forwarded by the E_VN to the next modules for trust computation, depending upon the nature of TM.

D. Data-Centric Trust Computation

This module supports TMs that compute trust on data rather than entity. In this module, trust is computed based on the quality of the received message (M_Q), which varies depending upon the message generated by the vehicle. If the transmitting vehicle has a direct link to the event, then higher trust value is assigned to the vehicles located within the close proximity of event. This trust value decreases with the increase in the distance from the event. However, if the transmitting vehicle has no direct link to the event, then indirect trust ($Trust_{ind}$) is calculated based on broadcast/drop (B/D) ratio:

$$Trust_{ind}(a, b) = \frac{Broadcast(a, b)}{Broadcast(a, b) + Drop(a, b)} \tag{2}$$

where, $Broadcast(a, b)$ and $Drop(a, b)$ are the number of broadcast and drop packets by the vehicle. Higher the B/D ratio, higher the trust value of the transmitting vehicle is. The high-level view of data-centric trust computation is depicted in Fig. 2.

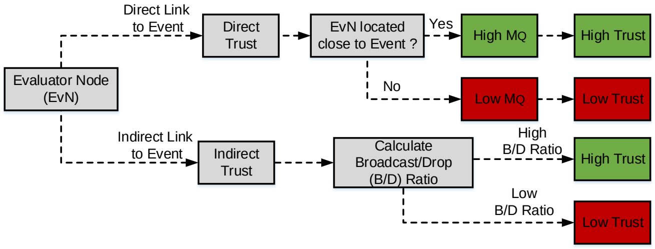

Fig. 2. Data-Centric Trust Computation

E. Node-Centric Trust Computation

In order to compute trust on the node, this module integrates two specific types of trust computation methods. (1) Role-oriented trust (ROT), and (2) Experience-oriented trust EOT. Every network incorporates vehicles which can be highly trusted, such as police vehicles, public buses, taxis, and ambulances—trusted vehicles ($Veh_{Trusted}$). ROT refers to such vehicles, where high trust can be assigned to messages generated by these vehicles. However, the major portion of the network disseminate messages generated by ordinary vehicles ($Veh_{Ordinary}$). These will include both legitimate and misbehaving vehicles. Therefore, to identify and distinguish messages generated by these vehicles, EOT is calculated. Trust level of the transmitting vehicle is increased for legitimate vehicles and is decreased for misbehaving vehicles. Node-centric trust computation is given as:

$$Trust_{nc} = \begin{cases} ROT & if veh = Veh_{Trusted} \\ EOT & if veh = Veh_{Ordinary} \end{cases} \tag{3}$$

In this work, we considered that 5% of the vehicles are performing ROT, while 95% vehicles are based on EOT.

F. Trust Evaluation

Once, data-centric and node-centric trust are computed, the next step involves the evaluation of these TMs via our trust evaluation platform. In order to evaluate trust, we consider several realistic trust evaluation criteria which we proposed in our previous work [18]. However, for the demonstration of our proposal in this work, we considered four specific trust evaluation criteria as it can exactly provide the information about the accuracy of the TM. These criteria include (1) false positive rates, (2) precision, (3) recall, and (4) F-measure.

III. Details of Implemented Trust Models

In this section, we present the three TMs (ETM, DTM, CTM) which we implemented to validate our proposal.

A. ETM

In order to validate our proposal, we implemented a multi-faceted based TM which is proposed by Minhas et al. [19]. This TM relies on four sources for the trust computation. This includes the experience of the message generator, their role & priority, and majority opinions of the participating vehicles. In this TM, the $E_V N$ shares messages with the prioritised vehicles within its vicinity and then awaits for the validity of the received messages. The prioritised vehicles validate messages based on two significant factors, i.e., (1) time closeness and (2) location closeness of the messages. This information is then shared with $E_V N$ in the form of opinions, where a majority opinion is done on the received opinions from the neighbours. $E_V N$ accepts messages only if the majority of the vehicles validate the trustworthiness of the messages. Otherwise, $E_V N$ follows the advise of the vehicle having highest role in the network. Further, $E_V N$ provides an honesty reward (ψ) to vehicles providing true report about the event and punishment (ρ) to vehicles providing malicious content.

In this work, we used a condition that trust is very hard to gain, therefore, we assigned higher weights to ρ, i.e., $(\rho/\psi = 10)$.

B. DTM

To validate our framework, we implemented a DTM, where trust by the $E_V N$ is calculated via two mechanisms, i.e., (1) Direct trust (T_D) and (2) Indirect trust (T_I) [20].

1) T_D: relies on the quality of the message (M_Q). Further $E_V N$ maintains a minimum threshold level for trust which must be satisfied by every vehicle. Moreover, when a vehicle provides trusted and true messages, the trust level of that specific vehicle is incremented by an honesty reward (ψ). For messages received from misbehaving vehicles, $E_V N$ decreases the trust level with the punishment factor (ρ).

2) T_I: is, on the other hand, calculated based on the message forward capability of the sending vehicle (V_S). Therefore, DTM calculates T_I based on Equation 2. The highest trust is assigned to vehicles which are broadcasting a high number of trusted messages. This level decreases as soon as the vehicle starts to drop the messages. Once, T_D and T_I are identified, $E_V N$ calculates the overall trust on V_S via Equation 4

$$Trust_{(E_V N, V_S)}(t) = \sqrt{Trust_{(E_V N, V_S)}(t-1) \times \sqrt{T_D \times T_I}} \tag{4}$$

$E_V N$ accepts messages only if the overall trust is above trust threshold. Otherwise, it discards the messages and categorised the vehicle as malicious and misbehaving.

C. CTM

To validate our proposal, we implement an event-oriented TM, known as Vehicular Security through Reputation and Plausibility checks (VSRP) [21]. As the name suggests, this TM highly rely on the reputation of the vehicles for trust computation. In this TM, neighbours are first identified by

$E_V N$ for initial evaluations using broadcast packets. $E_V N$ only accepts messages from the neighbours if a non-zero entry is available in its trust table. Next, $E_V N$ calculates trust on the messages received from such neighbours based on two parameters. (1) threshold range, and (2) detection range. If neighbour lies outside the threshold range, then $E_V N$ discards messages from such neighbours directly, assuming it to be malicious. However, for a message to be received from vehicles located within threshold range, then $E_V N$ performs second check on its detection range. In the detection range, $E_V N$ has a direct line-of-sight to the event. Therefore, any message which contradicts the $E_V N$ opinion is categorised as malicious and it is discarded and the trust level is decreased with a punishment factor ρ. The message is accepted only if the neighbour agrees with $E_V N$ by providing correct information, as a result, trust is increased with an honesty factor (ψ).

IV. Performance Evaluation

A. Simulation Scenario

The proposed trust evaluation mechanism is implemented in OMNET++ [22] and VEINS [23], [24], which is a widely used open source framework, is adopted for modelling VANET. We validated our proposal on a real map from the city of Derby, United Kingdom which we extracted from OpenStreetMap [25] as shown in Figure 3. Further, we relied on SUMO [26], [27] to generate traffic on this map, where we generated mobility of 100 vehicles. Moreover, we equipped all the vehicles with standard IEEE 802.11p communication module to enable them to communicate and share event (i.e., accident) information with each other.

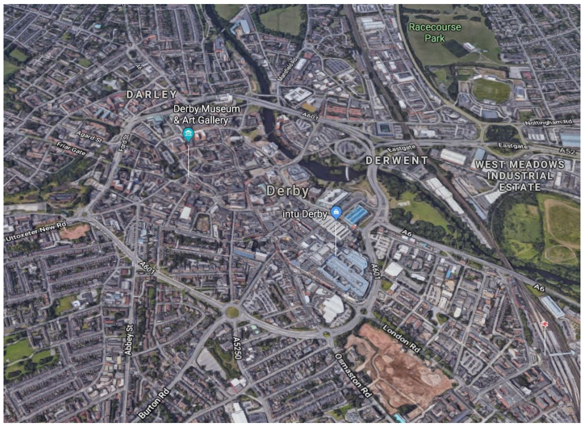

Fig. 3. Simulated Map of Derby, United Kingdom

Since the scope of this research work is to evaluate the performance of TMs in VANET under adversarial conditions, we have considered on-off attacks which can act as man-in-the-middle to drop and delay transmitted packets. In order to facilitate our simulations, we introduced 10% attackers and we then increased their proportion to 80% with a step of 10%. This mechanism will allow us to study the efficiency of TMs under both low and high quantity of malicious nodes. Further important details are highlighted in Table I.

TABLE I
Simulation Details

Parameters	**Details**
Total Simulation Time	1000 seconds
Simulation Area	4km × 2.5 km
Total No. of Vehicles	100
Total No. of RSUs	5
Total No. of Malicious Nodes	10%, 20%, ... , 80%
MAC Protocol	IEEE 802.11p
Network Protocol	IEEE 1609.4 (WAVE)
Packet Size (Data + Header)	1280 (1024 + 256) bits
Initial Trust	0.5
Trust Threshold	0.5
Honesty Factor (ψ)	0.01
Punishment Factor (ρ)	0.1

We executed every simulation scenario twenty-five times with random speed value to ensure the unique initial assignment of every vehicle within the network. Moreover, each simulation results are presented as an average of twenty-five runs for each simulation scenario.

B. Evaluation Metrics

To evaluate the efficiency of TMs via our proposal, we considered the following four metrics:

1) False Positive Rate (FPR): FPR illustrates the ability of the TMs to identify those misbehaving nodes which are incorrectly identified as legitimate nodes. Hence, FPR represents the error margin within the TMs. Ideally, the TMs with low FPR values are suggested in VANET due to the involvement of critical and sensitive information [28]. Let $P_{M|H}$ describes the probability of detecting vehicle as misbehaving, given the vehicle is honest, and $P_{H|H}$ is the probability of detecting vehicle as honest, given the vehicle is honest, then FPR is expressed as:

$$FPR = \frac{P_{M|H}}{P_{H|H} + P_{M|H}} \tag{5}$$

2) Precision: Precision is widely used to calculate the accuracy in information retrieval [6], [29]. Let $P_{M|H}$ represents probability to detect node as malicious, given legitimate node and $P_{M|M}$ is the probability to detect node as malicious, given malicious node, then precision is given as:

$$Precision = \frac{P_{M|M}}{P_{M|H} + P_{M|M}} \tag{6}$$

3) Recall: Recall, on the other hand, is also an important parameter within information retrieval to calculate its accuracy [6], [29]. Recall identifies the capability of TM to correctly detect misbehaving nodes. Let $P_{M|M}$ presents the probability of TM to detect node as malicious, given node is malicious and $P_{H|M}$ resents probability of detecting malicious node as legitimate node, given the node is malicious, then Recall can be mathematically expressed as:

$$Recall = \frac{P_{M|M}}{P_{H|M} + P_{M|M}} \tag{7}$$

In this paper, both Precision and Recall values are calculated in order to identify accuracy level of the TM to correctly identify misbehaving nodes.

4) F-Measure: F-Measure, a weighted average of precision and recall is an important metric which can evaluate the accuracy of the TMs [30]. The higher the F-Measure, the higher accuracy of the TM. F-Measure can be mathematically given as:

$$F - Measure = 2 \times \frac{Precision \times Recall}{Precision + Recall} \tag{8}$$

V. Simulation Results

The accuracy of the TMs is depicted in Figs. 4 to 6 in terms of precision, recall and F-measure. It clearly depicts that when we increase the number of malicious nodes in the network, precision, recall and F-measure decreases significantly. Precision of the TMs is depicted in Fig 4, stating that for low number of malicious nodes, all the TMs can detect malicious content generated by these malicious nodes as the precision achieved is over 90%. However, this precision decreases below 85% when high number of malicious nodes are introduced in the network. Further, ETM achieves higher precision values than DTM and CTM. For a network with 50% malicious nodes, ETM achieves 10.8% and 5.7% precision values than DTM and CTM respectively. This is due to the ironic nature of ETM where trust is computed via ROT and EOT. These methods (ROT and EOT) ensure that the malicious nodes are identified correctly in the network.

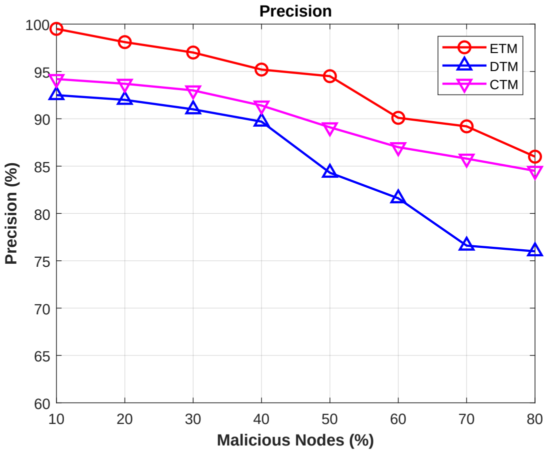

Fig. 4. Precision

Similarly, recall of the TMs is given in Fig. 5, stating that with the injection of malicious nodes in the network, the ability of the TMs to truly detect actual misbehaving nodes decreases. This is due to the fact that the high number of malicious nodes can compromise the integrity of the messages and hence they can dominate the network and the legitimate nodes. Further, Fig. 5 suggests that ETM performs better than both DTM and CTM in terms of recall. Specifically, ETM achieves 5.88% and 4.4% higher recall values than DTM and CTM respectively when the network is simulated with 50% malicious nodes.

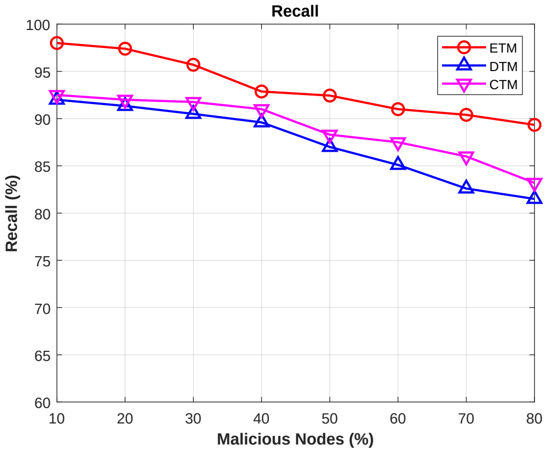

Fig. 5. Recall

Finally, Fig. 6 identifies an important metric to evaluate TMs, i.e., F-measure. Since, previous metrics suggested that the distribution of malicious nodes in the network can affect the performance of VANET, therefore, this metric is helpful to understand how accurate the TM is in identifying malicious nodes and their content. Fig. 6 further depicts that in terms of F-measure, ETM can accurately identify true content in presence of high number malicious nodes, i.e., ETM is 8.37% and 5% more accurate than DTM and CTM when the network contains 50% malicious nodes. This is due to the presence of vehicles with highest roles and experience in the network which have the ability to identify malicious nodes and the content they generate.

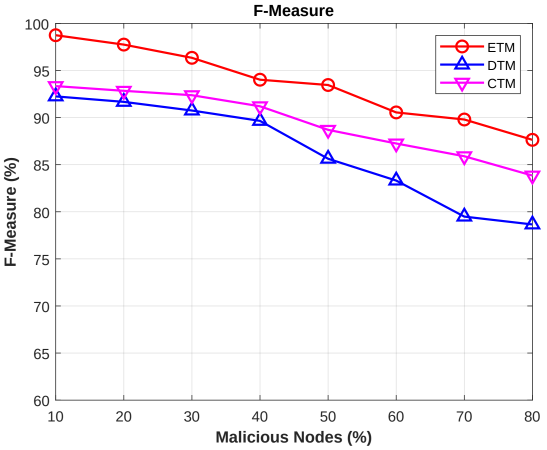

Fig. 6. F-Measure

Figure 7 represents the false positive rate (FPR) for three TMs (ETM, DTM and CTM). As stated earlier, the FPR for the TMs should be at minimum level in VANET. Figure

7 depicts that all the TMs achieve low FPR even if the network is polluted with high number of malicious nodes. However, comparing the three TMs in terms of FPR, we can see that ETM outperforms both DTM and CTM where FPR is maintained at minimum level. For a network with 50% adversaries, ETM achieves about 27.2% and 55.45% better FPR values than DTM and CTM respectively. This is due to the fact that ETM relies on both ROT and EOT for trust computation, thus increasing the probability of detecting high number of false positives in the network. On the other hand, DTM and CTM evaluates trust on data, which can be compromised by adversaries, thus, increasing the probability of propagating false positive across the network.

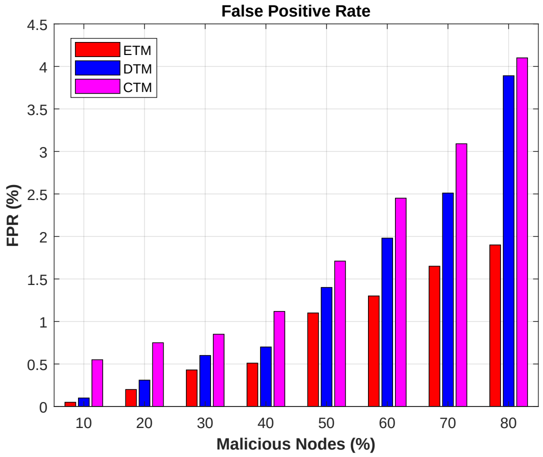

Fig. 7. False Positive Rate

VI. Conclusion

We have presented various trust models (TMs) for VANETs which are broadly categorised into three categories, namely entity-oriented (ETM), data-oriented (DTM) and combined trust models (CTM). These TMs evaluate trust on the data or on the entity or both via different mechanisms. Our research provided a mechanism to evaluate these TMs in term of security and trust, where the accuracy of the TMs is evaluated in terms of misbehaving nodes and faulty information dissemination under different scenarios. Our paper has identified the capabilities and the limitations of each simulated TM. It was clear that the ETM outperformed DTM and CTM on different criteria, due to the use of (1) Role-oriented trust (ROT), and (2) Experience-oriented trust (EOT) for trust computation. These metrics seem to reflect real applications/scenarios and should be considered for further development in VANET. The results and the analysis could be used for further development of TMs and improvement of existing models.

References

[1] Y. Mehmood, F. Ahmad, I. Yaqoob, A. Adnane, M. Imran, and S. Guizani, "Internet-of-Things Based Smart Cities: Recent Advances and Challenges," *IEEE Communications Magazine*, vol. 55, no. 9, pp. 16–24, 2017, doi: 10.1109/MCOM.2017.1600514.

[2] F. Ahmad, C. A. Kerrache, F. Kurugollu, and R. Hussain, "Realization of Blockchain in Named Data Networking-Based Internet-of-Vehicles," *IT Professional*, vol. 21, no. 4, pp. 41–47, July 2019.

[3] J. Wang, Y. Shao, Y. Ge, and R. Yu, "A Survey of Vehicle to Everything (V2X) Testing," *Sensors*, vol. 19, no. 2, 2019, doi:10.3390/s19020334.

[4] F. Sakiz and S. Sen, "A Survey of Attacks and Detection Mechanisms on Intelligent Transportation Systems," *Ad Hoc Networks*, vol. 61, pp. 33–50, 2017.

[5] F. Ahmad, A. Adnane, V. N. L. Franqueira, F. Kurugollu, and L. Liu, "Man-in-the Middle Attacks in Vehicular Ad-Hoc Networks: Evaluating the Impact of Attackers' Strategies," *Sensors*, vol. 18, no. 11, 2018, doi:10.3390/s18114040.

[6] W. Li and H. Song, "ART: An Attack-Resistant Trust Management Scheme for Securing Vehicular Ad Hoc Networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 17, no. 4, pp. 960–969, April 2016.

[7] T. Gazdar, A. Belghith, and H. Abutair, "An Enhanced Distributed Trust Computing Protocol for VANETs," *IEEE Access*, vol. 6, pp. 380–392, 2018, doi:10.1109/ACCESS.2017.2765303.

[8] S. Oubabas, R. Aoudjit, J. J. Rodrigues, and S. Talbi, "Secure and Stable Vehicular Ad Hoc Network Clustering Algorithm based on Hybrid Mobility Similarities and Trust Management Scheme," *Vehicular Communications*, vol. 13, pp. 128–138, 2018, doi:10.1016/j.vehcom.2018.08.001.

[9] A. Tolba, "Trust-Based Distributed Authentication Method for Collision Attack Avoidance in VANETs," *IEEE Access*, vol. 6, pp. 62 747–62 755, 2018, doi:10.1109/ACCESS.2018.2875906.

[10] C. A. Kerrache, N. Lagraa, C. T. Calafate, and A. Lakas, "TFDD: A Trust-based Framework for Reliable Data Delivery and DoS Defense in VANETs," *Vehicular Communications*, vol. 9, pp. 254–267, 2017, doi:10.1016/j.vehcom.2016.11.010.

[11] F. Ahmad, A. Adnane, C. A. Kerrache, V. N. L. Franqueira, and F. Kurugollu, "Trust Management in Vehicular Ad-Hoc Networks and Internet-of-Vehicles: Current Trends and Future Research Directions," in *Global Advancements in Connected and Intelligent Mobility: Emerging Research and Opportunities*, F. Outay, A.-U.-H. Yasar, and E. Shakshuki, Eds. IGI Global, 2019, pp. 135–165, doi:10.4018/978-1-5225-9019-4.ch004.

[12] Z. Lu, G. Qu, and Z. Liu, "A Survey on Recent Advances in Vehicular Network Security, Trust, and Privacy," *IEEE Transactions on Intelligent Transportation Systems*, vol. 20, no. 2, pp. 760–776, Feb 2019, doi:10.1109/TITS.2018.2818888.

[13] C. A. Kerrache, N. Lagraa, R. Hussain, S. H. Ahmed, A. Benslimane, C. T. Calafate, J. Cano, and A. M. Vegni, "TACASHI: Trust-Aware Communication Architecture for Social Internet of Vehicles," *IEEE Internet of Things Journal*, pp. 1–1, 2019.

[14] F. Ahmad, A. Adnane, F. Kurugollu, and R. Hussain, "A Comparative Analysis of Trust Models for Safety Applications in IoT-enabled Vehicular Networks," in *11th IEEE Wireless Days (WD)*. IEEE, April 2019.

[15] A. Mehmood, B. Butler, W. E. Zhang, Q. Z. Sheng, and S. A. Siddiqui, "A Hybrid Trust Management Heuristic for VANETs," in *PerVehicle'19 - 1st International Workshop on Pervasive Computing for Vehicular Systems*. IEEE, 2019, pp. 748–752.

[16] European Telecommunications Standards Institute, "Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service, ETSI TS 102 637-2," ETSI, Tech. Rep., 2011.

[17] S. Biswas and J. Mišić, "Establishing Trust on VANET Safety Messages," in *International Conference on Ad Hoc Networks (ADHOCNETS)*. Springer, 2010, pp. 314–327.

[18] F. Ahmad, J. Hall, A. Adnane, and V. N. L. Franqueira, "Faith in Vehicles: A Set of Evaluation Criteria for Trust Management in Vehicular Ad-hoc Network," in *Proceeding of the IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, June 2017, pp. 44–52.

[19] U. F. Minhas, J. Zhang, T. Tran, and R. Cohen, "A Multifaceted Approach to Modeling Agent Trust for Effective Communication in the Application of Mobile Ad Hoc Vehicular Networks," *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)*, vol. 41, no. 3, pp. 407–420, May 2011.

[20] C. A. Kerrache, C. T. Calafate, N. Lagraa, J. C. Cano, and P. Manzoni, “Trust-Aware Opportunistic Dissemination Scheme for VANET Safety Applications,” in *International IEEE Conferences on Ubiquitous Intelligence Computing, Advanced and Trusted Computing, Scalable Computing and Communications, Cloud and Big Data Computing, Internet of People, and Smart World Congress (UIC/ATC/ScalCom/CBDCom/IoP/SmartWorld)*. IEEE, July 2016, pp. 153–160.

[21] S. K. Dhurandher, M. S. Obaidat, A. Jaiswal, A. Tiwari, and A. Tyagi, “Vehicular Security Through Reputation and Plausibility Checks,” *IEEE Systems Journal*, vol. 8, no. 2, pp. 384–394, June 2014, doi:10.1109/JSYST.2013.2245971.

[22] OMNET, “OMNET++: Discrete Event Simulator,” available online: https://omnetpp.org/ (Accessed: 29th January, 2019).

[23] Veins, “Vehicles in Network Simulation, The Open Source Vehicular Simulation Framework,” available online: http://veins.car2x.org (Accessed: 29th January, 2019).

[24] C. Sommer, R. German, and F. Dressler, “Bidirectionally Coupled Network and Road Traffic Simulation for Improved IVC Analysis,” *IEEE Transactions on Mobile Computing*, vol. 10, no. 1, pp. 3–15, January 2011.

[25] OpenStreetMap, “OpenStreetMap,” Available online: https://www.openstreetmap.org (Accessed: 29th January, 2019).

[26] SUMO, “Simulation of Urban MObility,” Available online: https://sumo.dlr.de/ (Accessed: 29th January, 2019).

[27] M. Behrisch, L. Bieker, J. Erdmann, and D. Krajzewicz, “SUMO-Simulation of Urban Mobility: An Overview,” in *Proceedings of the Third International Conference on Advances in System Simulation*, 2011.

[28] F. Ahmad, V. N. L. Franqueira, and A. Adnane, “TEAM: A Trust Evaluation and Management Framework in Context-Enabled Vehicular Ad-Hoc Networks,” *IEEE Access*, vol. 6, pp. 28 643–28 660, May 2018, doi: 10.1109/ACCESS.2018.2837887.

[29] J. Davis and M. Goadrich, “The Relationship Between Precision-Recall and ROC curves,” in *Proceedings of the 23rd international conference on Machine learning*. ACM, 2006, pp. 233–240.

[30] Y. M. Chen and Y. C. Wei, “A Beacon-Based Trust Management System for Enhancing User Centric Location Privacy in VANETs,” *Journal of Communications and Networks*, vol. 15, no. 2, pp. 153–163, April 2013.