Chapter 6

Distributed Trust and Reputation Mechanisms for Vehicular Ad-Hoc Networks

Marcela Mejia and Ramiro Chaparro-Vargas

Additional information is available at the end of the chapter

http://dx.doi.org/10.5772/55453

1. Introduction

The parallel evolution of automotive industry and anywhere/anytime communication mechanisms has defined a revolutionary moment for intelligent driving concept. Vehicular Ad Hoc Networks, also known as VANETs, exploit the capability of wireless communications protocols to confidently disseminate sensitive information among peers, restricted to a particular geographic area, as well as the advanced safety-assets, on road sensors and sophisticated driving-assistance features of top-generation vehicles. Such a complement are not only oriented to offer a more pleasant in-car experience for driver and passengers, but also are intended to introduce autonomous and efficient ways to prevent hazardous situations on roads. Then, VANETs deployment should follow a primary task based on reliable message handling for sharing traffic conditions, weather variables, driving assistance, navigation support, entertainment content multicasting and even spurious notifications [1], [2].

Regarding some previous approaches over vehicular networks, Vehicle to Infrastructure (V2I) and Vehicle-to-Vehicle (V2V) are two well-know concepts for their implementation [3], [4]. The former claims for a centralized control entity dedicated to information processing and decision making. Although, given the dynamic nature of the involved communications nodes, the ubiquity along the road becomes a mandatory requirement. This might implies a high-affordable effort, due to the demanded deployment of extended communication infrastructure road-sided [5].

On the other hand, the introduction of inter-vehicle communication takes advantage of partially decentralized and self-controlled characteristics from mobile nodes. Such a distributed scenario forms an interim delegation of controlling role, while the privilege to command the network is granted based on the possession of sensitive information to be shared among peers. Correspondingly, V2V communication inherits typical performance

hurdles and security threats from distributed mobile networks [6], [7]. Consequently, particular attention should be given to node authenticity, message integrity and reputation features, aiming to promote an integral trust solution [8]. Since an important set of messages contains critical information for the vehicles involved, selfish or malicious behavior should be diminished as possible. On this way, strategies conducted in Mobile Ad Hoc Networks (MANETs) research context are prone to be addressed in VANETs setups as well [9], in order to contrast results from real and simulated scenarios regarding native vehicular network protocols and ad hoc networks' tailored approaches.

The present chapter is dedicated to the review of trust and reputation models for VANETs from different technical, technological and performance perspectives. Besides, novel approaches are introduced, given their capabilities to tackle some of drawbacks and downsides of current approaches [10].

The achievement of trustworthiness among peers infers some inherent challenges owing to vehicles' high speeds and ephemeral associations. For this reason, an initial key issue is directed to guarantee the verification and processing of incoming information in a real-time basis. Likewise, the large population of automobiles in urban streets or suburbs highways at specific time periods affects network channel saturation. Then, some efforts should be oriented to turn the implicit protocols into scalable mechanisms and selective message forwarding. Moreover, VANETs' dynamic properties lead to assume the necessity of decentralized and self-controlled infrastructures appealing to unique and short-term acquaintances among peers. However, hybrid or combined models are subject of discussion in the upcoming sections as feasible VANETs environments. Additionally, VANETs incidents can be distinguished as informational, warning and critical events; in any case spatiotemporal descriptors (i.e. location and time tags) must be properly processed according to priority, life span and certainty aspects. Finally, the adoption of mobility models is directly related with the efficiency of the trust and the reputation system, whereas the accuracy degree of transit patterns influences simulations' results and further implementations in real scenarios [11].

The upcoming sections discuss some remarks on trust and reputation management systems, as well as, trustworthiness models based on diverse mechanisms for scalability, privacy, entity management, content reputation, forwarding, rewarding and so on. Afterwards, innovative models are described in order to establish their original contributions for challenges overthrowing and general VANETs development.

2. Trust and reputation for VANETs in scope

Pursuing multi-featured trust and reputation models, issues of scalability, security, performance and sustainability should be addressed in VANETs. Inasmuch as multi-featured trust and reputation models are pursued, topics from generalization, security, performance and sustainability are addressed. The following criteria enclose the requirements and guidelines in order to accomplish outstanding trust and reputation models [12], [13].

2.1. Low complexity

The interactions among VANETs' peers are characterized by a circumstantial occurrence at high speeds and short time periods (ephemeral acquaintances). During this timeframe, the sender automobile should transfer reliable information within its influence radius. The

http://dx.doi.org/10.5772/55453

computation of trust and reputation metrics should be executed by the master algorithm under low complexity constraints, i.e. cost-efficient processing, fast-access memory, improved transmission rates and effective throughput.

Hardware and software specifications related to processing and storage are conceived not only to fulfill single-threaded duty cycles at high frequencies, but also to support eventual burst of messages from different sources at given time instants. Similarly, data transmission rates need to rely on recognized standards and specifications in charge of modulation schemes, media access and packet routing. Even so, the overhead linked to the throughput portion should be kept at minimum, since excessive encode/decode of protocols headers leads to critical delays for the reception of meaningful driving information.

2.2. Scalability

Scalability should be understood as a fundamental condition for a trust and reputation mechanism in any application. Moreover, the occurrence of incidents or events on the road could be triggered by multiple mobile nodes, as well as single or minor set of vehicles. Either way, the system should be prepared to conveniently process any incoming information at bursting rates, preventing increased packet drop or perceptible latency at decision time.

An initial approach implies the improvement of system's physical capabilities to handle plenty of concurrent messages, and thus, reducing the probability of missing messages or extended processing cycles for warnings and alerts posting. In general, the fulfillment of requirements by the overestimation of resources seems to be the most immediate, but rarely, the most efficient solution. Therefore, alternative methods should be employed to chase model's top-performance, while low complexity and simplicity are preserved. For instance, solutions based on reputation records could allow selective forwarding and reception of incoming and outcoming information, respectively. So that resources are allocated to nodes that have displayed a good behavior within the network. Of course, prerequisites must be taken into account to promote the success of this model; such as precedent behavior awareness and reputation history access. Balance-oriented solutions claim for fair resources disposal, accompanied by the definition of conservative thresholds around incoming packets upper limits, relay nodes allowance and messages intervals designation.

2.3. Sparsity

Some VANETs' environments can be described as dense populations of vehicles confined to relatively tight geographic areas, e.g. peak hours in urban zones. Other environments, like interstate or international highways are characterized by extensive trails with minimal density of automobiles. This situation makes difficult the application of multihop routing protocols from sources of events to spots of interest. Consequently, trust and reputation models should not be based on the evaluation of peer interactions, such as lists of relay nodes and reputation scorecards. Instead of this, these models should take into account the scarcity of information in the VANET. So, decision making algorithms and thresholds settings need to be as flexible as possible to process these messages. Even more, they should provide valuable data to the onboard driver and eventual adjacent mobile nodes, instead of attempting an unbiased execution of the trust and reputation mechanism.

2.4. Security and privacy-related

Undoubtedly, the extension of a security middleware for VANETs is understood as a major concern, relaying either on centralized or distributed schemes. Generally, every different approach aims to shield the communication infrastructure against potential security threats and vulnerabilities [14]. For example, one usual threat is represented by malicious mobile nodes, which might attempt to disseminate false or corrupted information by making use of resources and the communication channel, perversely. Dissimilarly to other network contexts, misbehavior of a single node might imply severe or even lethal consequences to benign peers; whereas the injection of deceiving content is prone to conclude in inattention of vital recommendations or commitment of undesired actions. The author Zhang in [13] describes some common attacks that represent a critical challenge for trust and reputation mechanisms. Some of them are briefly introduced as follows.

- Newcomer Attack: Specially applied by mobile nodes with an undesirable cooperative behavior. By the registration of a new identity in the trust and reputation system, the malicious node attempts to delete its negative history to gain the attention of adjacent nodes as a freshman.
- Sybil Attack: Consists of creating multiple and fake identities (pseudonyms) by a single malicious entity. Thereafter, a pass-through is granted to the false information by pretending peers, who attempt to detour network resources to their own benefit or collapse general message distribution.
- Betrayal Attack: Appealing to a hypocrite strategy, a malicious peer formidably cooperates within the network until high reputation and trust scores are received. Suddenly, its behavior turns inadequate by propagating deceiving content, while it takes advantage of the influence over the mobile neighbors.
- Inconsistency Attack: Related to the previous attack, a vehicle oscillates between benign and malicious behavior at different periods of time. The intention of this attack seeks to destabilize the trust and reputation mechanism by entering chaotic records to the observed interaction among mobile nodes.
- Collusion Attack: Also known as conspiracy attack, a group of malicious peers subscribes a dishonest coalition to generate false information to the network from multiple points. Keeping relatively outnumbered agents, the attack may also affect or even collapse the content distribution system among vehicles.
- Bad-mouthing/Ballot Stuffing Attack: Following the line of conspiracy attacks, a set of malicious nodes gains access to the network with a cooperative behavior. Once, rating or feedbacks about other adjacent peers are requested, inaccurate opinions are provided. Attempting to unfairly increase reputation of suspicious nodes (ballot stuffing) or unfairly decrease reputation of benign entities (bad-mouthing).

Defense mechanisms for the aforementioned attacks are regarded from the universal framework of information security for general data networks [15], including AAA protocols, symmetric, asymmetric systems, cryptographic key management, etc. However, absolute solutions have not still been met; e.g. the absence of key distribution mechanisms may lead to the interception of shared secrets by unauthorized entities in symmetric key deployments. On the other hand, the asymmetric cryptosystems may compromise the public keys'

http://dx.doi.org/10.5772/55453

distribution by sophisticated techniques of replacement or theft of network identities and traffic information. Therefore, keys authenticity assurance turns into a vital security matter. So, the deployment of credentials, from now on called certificates, allow us to bind the public key to the owner's name and a trusted third party, designated as Certificate Authority (CA). Of course, the generation, management and revocation of certificates may become a complex endeavor when the number of network entities tends to increase. For this reason, a Public Key Infrastructure (PKI) rises as a solution to handle major aspects, such as certificates' lifecycles, issuance, distribution, suspension and revocation. Although, further considerations should be applied to adapt PKI to a partial or total distributed topology in VANETs environment.

2.5. Independence of mobility patterns

Mobility pattern is a central point of the discussion about VANETs topologies. Even more, mobility pattern is a crucial issue in ad hoc networks research, given its direct relation with protocols, models and performance analysis. The definition of restrains for the transit, environment variables and interaction rules among entity nodes, determines a set of standard rules for a correct simulation and performance analysis of VANETs. In VANETs context, a group of mobility patterns has been proposed intending to assemble an universal playbook to guide the simulation of different vehicular models, including trust and reputation. Those patterns aim to set parameters related to automobiles density, traffic area, traffic lights and stop signs existance, average speeds, block and streets disposition, weather conditions, overtaking chances and any other variable that can emulate a real vehicular scenario [11].

Despite of being so attractive, the idea behind of a trust and reputation model entirely independent of mobility patterns, there are reasonable and heuristic assumptions that might lead to disregard this possibility. Instead of designing a unique trust and reputation model for any possible mobility pattern, major efforts should be conducted to adapt variations of the mechanism to consider some of the most recurrent patterns in urban or rural areas. Consequently, models' structure should include degrees of freedom that easily permit alternative resources allocation and algorithmic shortcomings, depending on detected transit, environmental and interaction parameters.

2.6. Trust and reputation decentralization

The distributed and self-controlled feature of VANETs is an extensively accepted concept, given the mobile-oriented dynamic of the nodes. Thus, lots of research works refer to message relay, security assurance, privacy adoption and trust/reputation establishment toward decentralized deployments. The interaction among peers is the base of trust and reputation construction [16]. Random peer-to-peer acquaintances allow the establishment of trustworthiness relationships by references at first hand, i.e. the definition of reliable nodes depends on direct observations by the sensor-equipped vehicle on road. It is expected to assign a greater confidence valuation to those nodes, once the event or incident is corroborated by an observer peer. Complementary, referral mechanisms are introduced to trust and reputation systems in order to optimize the convergence time and awareness status. That means, an interested node might request recommendations or opinions from adjacent nodes to assign a trust value to peers out of the scope. Also, it is expected to set a lower confidence degree to unreachable vehicles, ought to the lack of personal certainty about its reliability. Achieving a complete decentralization is not easy due to slow convergence,

delays in peer status update, network changes, etc. Indeed, the uncertainty about short-term or long-term encounters among vehicles hinders the assembling of trust information over the whole network. Because of this, there are proposals to introduce some controversial entities in VANETs, the Road Side Units (RSU). They would coordinate the gathering of information at infrastructure based concentration points, in a centralized approach. Due to a hard-wired interconnection (e.g. optic fiber rings), RSUs are capable to share information at significant transfer rates to be transmitted immediately to vehicles within their coverage. In spite of breaking apart the decentralization concept, coexistence of both mechanisms for trust and reputation establishment are still widely studied [17], [18].

2.7. Confidence measure

Even though, trust and reputation mechanisms have been able to carry on trustworthiness valuations successfully. Some additional metrics need to be applied, in order to introduce "Quality Assurance" (QA) into VANETs' models. The knowledge level about mobile peers may not be always associated to highly consistence databases, due to several facts. For example, minimum requirements for algorithm computation, lack of memory, unavailability of data or simply owners' and manufacturers' discretion.

For this reason, confidence measure stands out as a statistical QA parameter to assess the accuracy degree of modeled trustworthiness values [13]. A scoped vehicle makes use of this measure to decide how useful the incoming content could be, according to particular circumstances on the road. Such that, an automobile with low confidence measures about neighbors and events is encouraged to seek alternative referees to improve its levels of certainty; but the same vehicle who faces scarcity of information sources has no better option than supports its decision on the current confidence metric. Then, exactly the same parameter can be easily ignored at one particular situation and overvalued throughout in another.

2.8. Event description and spatiotemporal specification

There are various types of events to happen on roads, highways or even quiet urban lanes. The description level plays a fundamental role within trust and reputation models to assign weights and priority tags to incoming information, according to messages' description. The distinction among informational, warning and critical events needs to be clearly specified and managed by all peers. Not only to suggest a suitable action in consequence with the input data, but also to incentivize with proportional rewards to the forwarding nodes. It means, nodes that are willing to cooperate wisely with life-saving messages over meaningless broadcasting.

Likewise, location and time parameters exhibit further benefits in trustworthiness assessment than merely timestamps accounting features. High-dynamic essence of VANETs infers real-time spatiotemporal feedback about vehicles walk-through, expecting minor location and launching efforts of authorities, when incidents occur. Once a major event is reported, mobile nodes that are closer located and sooner reckoning might offer a greater accuracy of transmitted information, as well as, the kind of assistance required. In this case, advantageous geolocation of reporter nodes should be also treated with higher trust values and subsequently generous reputation scores should be awarded, if information is confirmed.

http://dx.doi.org/10.5772/55453

Summarizing, Table 1 depicts the criteria for trust and reputation models in VANETs with their corresponding current development status, according to the related research work.

Feature	Pending	In progress	Covered
Low Complexity		×	
Scalability			×
Sparsity	×		
Security and privacy-related		×	
Mobility patterns independent			×
Trust and reputation decentralization			×
Confidence measure	×		
Event and spatiotemporal specification			×

Table 1. Criteria for trust and reputation models in VANETs.

3. Discussion on trust and reputation models

At this point, a rich collection of challenges about trust and reputation modeling for VANETs has been introduced. Now, a review of existing mechanisms is prepared, attending to challenges, design criteria, implementation hurdles and support insights. Depending on particular VANET context, several models are explored, appealing to heterogeneous techniques over infrastructure, interaction and trustworthiness assessment matters. In what follows, we will review some of them.

3.1. Content Reputation System - CoRS

CoRS protocol is a content-based message reputation model, i.e. message content is the primary analysis object for trustworthiness computation [17]. Nevertheless, additional features are applied for node authenticity and information integrity based on cryptographic mechanisms. PKI infrastructure and threshold cryptography are the components employed by CoRS to assess reliability of mobile nodes, while the protocol focuses on content reputation, exclusively. The former demands a valid pair of cryptographic keys for each participant in the VANET, which are usually provided by the CA. The distribution of digital certificates includes a public and a private key, which are meant to establish a secure channel among peers for the exchange of messages. As long as ciphersuites are in charge of encoding and decoding tasks at each side. In the same manner, digital certificates are engaged to perform authentication procedures in order to validate peers' identity, as a first step.

On the other hand, the threshold cryptography system performs a critical role within the content reputation model. Despite of being an old-fashioned concept in information security literature, its validity remains quite bearable. The basic concept behind cryptographic threshold states a mechanism to divide into n chunks a whole data packet P, and then, a previous knowledge of c or more chunks will permit the complete packet P reconstruction [19]. But only, defining up to $c-1$ chunks will lead to a certain data undisclosed; so polynomial interpolation is applied to compute the initial threshold pair (c,n). From that, the theorem claims that given c different points on the two-dimensional plane, such that $(x_i,y_i)\ \forall\ i\ \in\ [1,c]$, one and only one polynomial $f(x)|f(x_i)=y_i$ with degree $c-1$ exists. The remaining chunks of the data packet P can be found with Equation 1

$$f(x) = a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \cdots + a_{n-1} x^{c-1} \quad (1)$$

where a_0 represents the whole data packet P and the other coefficients a_i are chosen randomly. To summarize, the definition of c chunks and their corresponding indices conducts to find the coefficients of $f(x)$ and recover data packet $P = f(0)$ by interpolation computation.

The threshold cryptography is applied in threshold signatures generation, which is the core machinery of trustworthiness assembly in CoRS. This cryptosystem introduces digital signatures for distributed environments by the usage of three major components: 1) a threshold public key K_{pub}, 2) a certificate C and 3) a key share K_{share}, which is a partial private key. Such that, only the combination of cooperative nodes with their respective K_{share} allows digital signature verification, and thus, content validation. The management of K_{share} is delegated on a CA or share dealer; which should cope with the determination of the minimum number of K_{share} required to successfully sign a message, as well as, at least one share delivery to each mobile node. Figure 1 shows players and workflow of threshold signature for distributed reputation systems.

Once, the share dealer has generated and distributed K_{share} among registered vehicles, a random combiner executes an algorithm to integrate partially signed data chunks; whose outcome produces a valid digital signature to sign the message. So, the resulting signature can be verified using the corresponding certificate, whilst individual shares are kept in secret during combination process. Figure 1 depicts the threshold signature procedure for CoRS protocol.

Having all the pieces into place, we will proceed to explain the involved phases in CoRS mechanism.

3.1.1. CoRS initialization

The CA or share dealer generates the required certificates (including public cryptographic key K_{pub}), and shares K_{share} for n mobile nodes. Attempting to avoid a constant reset of the system every time a new vehicle registers into a particular VANET context, the relation between the number of nodes and shares is kept $N_{nodes} \gg N_{shares}$. That implies, more than one automobile is using the same K_{share} to partially sign the message. Gathering those components, each mobile node is prepared to perform authentication, data protection and message integrity, before content reputation system is taking place.

3.1.2. CoRS implementation

The protocol starts to detect an event or incident at some mobile node, known as *generator* (stage 1). Before it sends an information message *msg*, some support data is requested from the nodes located in the *reputation area*; even though the adjacent nodes very likely detect the same event, they are denoted as *verifiers* (stage 2). Then, *generator* produces a reputation request, which is signed using its personal private key K_{priv} and it is sent to the *verifiers* with the message itself. At *verifier's* side, the reputation request is validated employing the cryptographic elements. Further, content is verified, trying to check the several pieces of

http://dx.doi.org/10.5772/55453

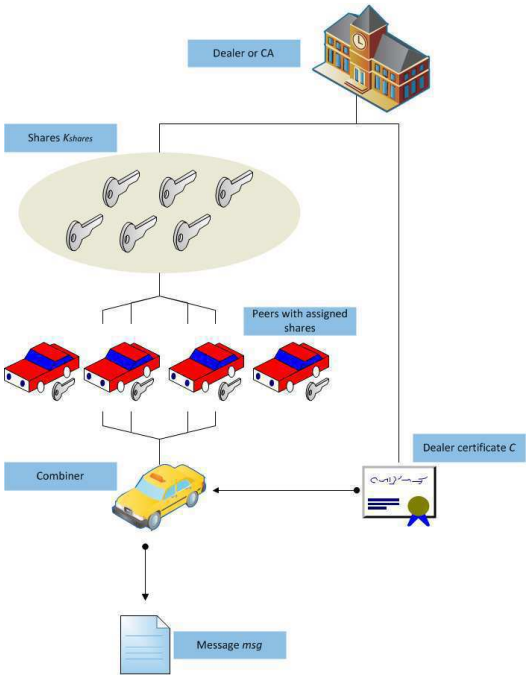

Figure 1. Threshold security for CoRS protocol.

information to evaluate the values for the reputation metrics r_m (stage 5). Such metrics serve to rate candidate events and message settings, depending on the most suitable category according to the following information.

- Event: In the case that the *verifier* has detected the same event as the *generator*, the former has the right to examine the message *msg* later. If not, the protocol workflow is terminated and the reputation request is not signed with its own K_{share}.
- Event detection time: The *generator* sets the message's timestamp as same as the event detection time. When the *verifier* receives a reputation request, its timestamp should not be larger than a predefined threshold, so only recent events are processed.
- Location of the event: The *verifier* determines the location of the event included in the reputation request, in order to define if it is identical to the incident observed by itself in its coverage area.
- Location of the node: To check the location of the *generator* in comparison with the potential *verifiers* and the event itself, a *collator* is required to resolve whether the distance is reasonably close.
- Sending time of the request: Eventually, a *collator* is not available at the sending time of the reputation request. Then, a second request will be transmitted with an implicit delay. The difference between event detection and sending time must handle some tolerance to allow further protocol computation.

Once, the reputation r_m information have been gathered to rate the trustworthiness level, a reputation computation is performed as follows.

$$Rep(msg) = \sum_{m \in \Re} r_m \tag{2}$$

For simplicity matters, unit-value scores are granted, i.e. +1 is given to affirmative validations, 0 for neutral and -1 for unsuccessful validations. While, $Rep(msg) \geq 0$ condition is fulfilled, the message *msg* is regarded as valid with a positive reputation and the *verifier* is set free to send a reply to the *generator*. Otherwise, the request reputation is neglected, turning the mobile node into a *denier*. The transmission of the reply message follows the same threshold cryptography guidelines, assuring authenticity and integrity by digital signing with K_{share} (stage 6). Furthermore, the *generator* collects all the incoming messages in order to validate digital signatures, and finds the information associated with the generated reputation request (stage 7). If all parameters of threshold signatures are hold (refer to section 3.1 introduction) (stage 8), the information message *msg* is distributed to other peers outside of the *reputation area* to let them know about the event or incident that is happening on the road.

As optional protocol's add-ons, broadcast manager (stage 3) and DoS protection (stage 4) help out to prevent broadcast storms and irregular content distribution, respectively. The former avoids reprocessing of already sent messages and the latter continuously check a list of banned peers, given its dishonest previous behavior.

The Figure 2 summarizes the stages involves in CoRS protocol workflow, based on player and general actions.

3.1.3. CoRS remarks

Despite of the reliance of CoRS protocol on central entities, the participation of central authorities or dealers represents a well-conducted and sustained strategy for node authentication, message integrity and data confidentiality. However, additional countermeasures are taken to avoid reiterative CA advisory, like threshold digital signature in a distributed mode. Though, the performance of different ciphersuites is not particularly discussed in CoRS framework; the protocol's workflow permits to infer a low complexity nature. By observing the protocol's pseudocode and involved stages, from event detection until information dissemination. CoRS preserves a balance between demand and consumption of resources [17].

Besides of this, threshold cryptography allows to improve scalability and sparsity, due to the bulky generation of shares among peers.

Nevertheless, it is possible for shares to collide during the normal execution of CoRS. Since, the number of nodes is always far greater than the number of shares, the possibility of assigning the same share to more than one automobile is quite plausible. Then, statistical modules may be needed to foresee encounter among peers with the same cryptographic signing material. Such a situation increases the complexity and time response of the general protocol. Owing to the distributed threshold cryptography, a compromising attack from

http://dx.doi.org/10.5772/55453

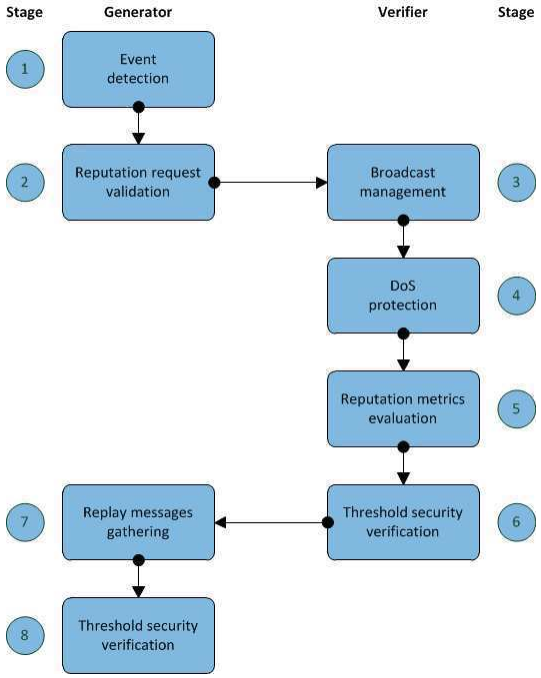

Figure 2. Content Reputation System (CoRS) workflow and stages [17].

one isolated node seems to be unfeasible. But, perverse coalitions among malicious peers (al least equivalent to the number of signing shares) will lead to successful collusion and bad-mouthing/ballot stuffing attacks. Finally, the existence of a role player, known as collator for location and time judging before ambiguities presence, it is more than necessary for the proper protocol walkthrough. Apparently, non-contingent policy is introduced to confidently step over or replace this sensitive requirement, so a high-faulty point is discovered.

3.2. Trust and Reputation Infrastructure-based Proposal - TRIP

TRIP protocol can be labeled as a hybrid trust and reputation model, whereas trustworthiness assessment is entity node- and content-oriented [20]. The decision making starts with a reputation score computation referred by three different possible sources: 1) directly acquainted mobile nodes, 2) referee nodes with indirect contact and 3) centralized authorities, like CA or RSU. Secondly, each mobile node is classified into three different trust levels, represented by fuzzy sets [12]. Considering, nodes' categorization further actions are committed. For instance, absolute data rejection (Not trust), data acceptance but not forwarding (+/- Trust) and message acceptance and forwarding (Trust). Finally, the information message is associated to a particular severity, priority or hazard. Only peers located in the highest trust level are allowed to transmit messages with the most critical severity. Similarly, peers settled in unfavorable trust levels will not find successful acceptance of any kind of message.

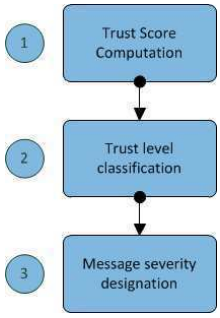

Figure 3. TRIP protocol workflow and stages.

3.2.1. Trust score computation

Let define v_i as the vehicle in charge of assessing a trust score for another vehicle v_j, which sends the message with a current situation on the road. As it was mentioned before, three different sources are empowered by TRIP protocol to issue a reputation score. Equations 3-5 denote the notation given to the calculation emitted by a direct peer, a referee node and a centralized entity, respectively.

$$\alpha_i * Rep_{ij}(t-1) \quad \forall \quad Rep_{ij} \in [0,1] \quad \alpha_i \in [0,1] \tag{3}$$

$$\beta_i \sum_{k=1}^{N} \omega_k * Rec_{kj} \quad \forall \quad Rec_{kj} \in [0,1] \quad \beta_i, \omega_k \in [0,1] \tag{4}$$

$$\gamma_i * Rec_{RSUj} \; \forall \quad Rec_{RSUj} \in [0,1] \; \gamma_i \in [0,1] \tag{5}$$

From Equation 3, a mobile node i has given a reputation score Rep about node j at a previous time instant $(t-1)$; and a tunable weight α_i is granted. Accordingly in Equation 4, a set of N peers indexed by k issues a recommendation Rec about node j, where ω_k represents the reliability of such referrals and β_i assigns a corresponding weight to the source. Finally, Equation 5 infers the recommendation value generated by RSU to a node j, accompanied by its weight γ_i. All the scores and weights are constrained to be allocated in the interval $[0,1]$. Merging the prior expressions, it is obtained the trustworthiness assessment for TRIP protocol, as shown in Equation 6.

$$Rep_{ij}(t) = \alpha_i * Rep_{ij}(t-1) + \beta_i \sum_{k=1}^{N} \omega_k * Rec_{kj} + \gamma_i * Rec_{RSUj} \quad \forall \; Rep_{ij} \in [0,1] \tag{6}$$

As soon as trust score is calculated, encouragements and punishments are scattered across the reputation area by the confirmation or denial of the reported event. The weights $\alpha_i, \beta_i, \gamma_i$ and reliability index ω_k are subject of increments and decrements, based on the accuracy level in the information disseminated by i^{th} and k^{th} peers at time instants t. Furthermore, the

http://dx.doi.org/10.5772/55453

identification of customary malicious nodes can be referred to central authorities or RSUs to compose a black list, which it is employed to ban spurious peers' participation with no further computations.

3.2.2. *Trust level classification*

The analytical value attained by Equation 6 leads to make a decision about the received information. According to the score, the message may be rejected, accepted but not forwarded, or accepted and forwarded. The authors in [12] proposed the fuzzy sets rendered in Figure 4 to associate trust levels and scores.

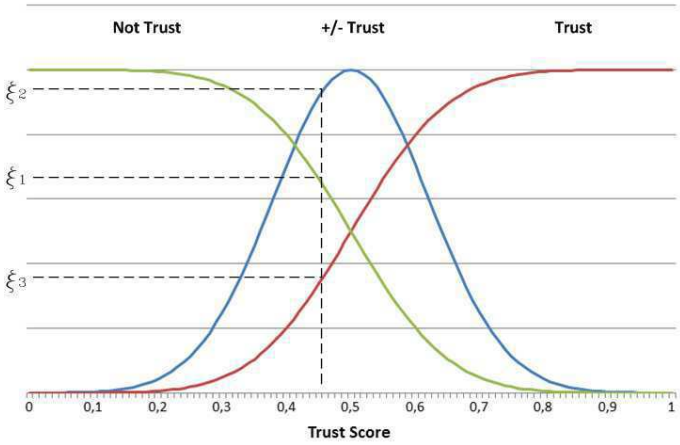

Figure 4. Fuzzy sets for trust levels [12].

To determine which trust level the automobile belongs to, each fuzzy set owns a membership function $\xi_F : F \rightarrow [0,1]$ (see Figure 4). Such that, the probability that a mobile node is placed in trust level TL_k is obtained by Equation 7.

$$P(TL_k) = \frac{\xi_k}{\xi_1 + \xi_2 + \xi_3} \quad \forall \ \xi_k = \xi_{TL_k}(Rep_{ij}(t)) \tag{7}$$

Given that a spotted vehicle is allocated in *Not Trust* region, its message is immediately neglected and one entry is entered in the black list managed by RSU. On the contrary, if the spotted vehicle is awarded in *Trust* set, its information is processed and shared with the nodes within the coverage area. The shadowing zone, labeled as +/- *Trust* supports message acceptance with no forwarding chance. However, the message acceptance is conditioned to an adaptable probability, designated as follows.

$$P_{+/-T} = \mu_{+/-T} - \mu_{NT} - \sigma_{NT} \tag{8}$$

where $\mu_{+/-T}$, μ_{NT} and σ_{NT} are the +/- *Trust* mean, *Not Trust* mean and *Not Trust* standard deviation, correspondingly. So, the higher $\mu_{+/-}$ becomes and the lower μ_{NT}, σ_{NT} tends, the higher the probability of acceptance $P_{+/-T}$ will be set.

3.2.3. Message severity designation

At the end, a certain severity level is given to each received message; which can be distinguished for important and hazard messages, information warnings and advertisement or less critical content. Therefore, Table 2 sums up the implicit relation between message classification and trust levels assigned to particular nodes.

Severity/Issued by nodes	Trust	+/- Trust	Not Trust
Hazard messages	×		
Information warnings	×	×	
Advertisement content	×	×	

Table 2. Acceptance of messages' severity with respect to trust levels.

3.2.4. TRIP remarks

TRIP protocol makes use of simple but well-assembled instruments in trustworthiness pursuing, by assessing trust scores with weighted polling strategies. Also, fair rewards and penalties are imposed to multilateral information sources, whilst the option of gaining higher rates is present, as long as peers interaction keeps in progress. Moreover, allocation of nodes and messages to different classification scales is based on tunable probabilistic functions, which might be adapted according to VANET context and observed nodes' behavior.

Unfortunately, no effort is intended to ensure the authenticity of the node, peers partial identification or pseudonyms avoidance. Even so, parallel research works in MANETs are proposed by the authors to cope with that. Therefore, the back door for newcomer and Sybil attacks is open, since the protocol by itself does not implement resilient mechanisms against them. In spite of integrating central entities or RSU as collaborative members for the query of malicious nodes' black list, the protocol manages to make of it a dispensable feature.

3.3. Data-Centric Trust Establishment framework - DCTE

For DCTE framework, trustworthiness establishment is sought through content analysis rather than entity nodes' identification. In paper [21], the authors claim: *"data trustworthiness should be attributed primarily to data per se, rather than being merely a reflection of the trust attributed to data-reporting entities"*. The derivation of trust and reputation metrics is focused on the amount of information that can be extracted from reported events. Likewise, multiple sources of evidence are taken into account to assign specific weights, in regard of inherent variables, such as geolocation or time occurrence. Consequently, original data and weighted metrics perform as input variables for a *decision logic* algorithm, which resolves a trust level output.

3.3.1. DCTE definitions

Before going through the details of event-reports evaluation or decision logic techniques, we will introduce some basic definitions for VANET environment contextualization.

http://dx.doi.org/10.5772/55453

- A set of mutually exclusive basic events, denoted as $\Omega = \{\alpha_1, \alpha_2, \alpha_3, \cdots, \alpha_I\}$ can be understood as traffic jam, slippery road, detour section, etc. Similarly, composite events $\Gamma = \{\gamma_1, \gamma_2, \gamma_3, \cdots, \gamma_I\}$ are the unions or intersections of basic events.
- A set of nodes or vehicles, expressed as $V = \{v_1, v_2, v_3, \cdots, v_K\}$ are classified following a system-specific set of node types, $\Theta = \{\theta_1, \theta_2, \theta_3, \cdots, \theta_N\}$. For consistency, let define a function $\tau : V \to \Theta$ to assign and return the type of a scoped vehicle v_k.
- Let set a *default trustworthiness* for a node v_k of type θ_n as a real value, depending on particular node attributes (e.g. onboard sensor equipment or on road authority member). Such that, every node type owns a unique and consecutive trustworthiness ranking, explained by $0 < t_{\theta_1} < t_{\theta_2} < t_{\theta_3} < \cdots < t_{\theta_N} < 1$.
- Let $\Lambda = \{\lambda_1, \lambda_2, \lambda_3, \cdots, \lambda_J\}$ be the set of tasks related to the protocol or system. Thus, two vehicles (v_1, v_2) with returned types $(\tau(v_1) = \theta_1, \tau(v_2) = \theta_2)$ and known default trustworthiness rankings $t_{\theta_1} < t_{\theta_2}$ are assumed, though it is still possible that v_1 is regarded as more reliable than v_2 in function of task $\lambda_j \in \Lambda$.
- Two input arguments, node type $\tau(v_k)$ and system task λ_j conform *event-specific trustworthiness* function, distinguished as $f : \Theta \times \Lambda \to [0, 1]$, which is invoked to differentiate among nodes of the same type when particular actions are required.
- In terms of security, let introduce *security status* function $s : V \to [0, 1]$, where $s(v_k) = 0$ means the revocation of the node v_k and $s(v_k) = 1$ infers the node legitimacy. Any intermediate value within the interval may be used to characterize scaled security levels.
- At last but not least, let set a *dynamic trust metric* function, expressed by $\mu_l : V \times \Lambda \to [0, 1]$. The index l points out dynamically changing attributes of nodes. Therefore, for every attribute, a corresponding metric μ_l is applied.

3.3.2. DCTE trustworthiness function

The computation of trustworthiness is data-centric or report-oriented. Also, the generated value from the j^{th} report e_k^j is provided by K distinct mobile nodes v_k, which supports on scattered evidence of event α_j. The integration of default trustworthiness, security status, node type and event-specific trustworthiness functions shapes a general trust function, denoted by Equation 9

$$F(e_k^j) = G(s(v_k), f(\tau(v_k), \lambda_j), \mu_l(v_k, \lambda_j)) \quad \forall \; F(e_k^j) \to [0, 1] \tag{9}$$

The obtained weights or trust levels within the interval $[0, 1]$ are assessed by a vehicle v_k with respect to every incoming event report from surrounding nodes. Since, the combination of multiple pieces of evidence is one major concern in DCTE, one unique weight is not a confident enough outcome. Henceforth, the composite of various weights related to the same event will conduct to a more robust and reliable decision material. Then, the reports accompanied by their matched weights are transferred to a *decision logic* module that manages to find a definitive action to be taken, like message disposal, conditioned forwarding or full-compliance.

3.3.3. DCTE decision logic

The decision logic module is strongly related to multisensor data fusion techniques. Hence, the performed algorithms are rule-based systems, matching simple polling [22], weighting [23] or statistical procedures. In DCTE context, bayesian inference (BI) and Dempster-Shafer theory (DST) are discussed as candidate data fusion techniques for decision logic implementation.

Bayesian Inference

BI is supported by the well-known Bayes' theorem, where the blended weight of a particular event α_i is defined by the *posteriori* probability of α_i given novel pieces of evidence, $e = \{e_1^j, e_2^j, e_3^j, \cdots, e_K^j\}$ and it is expressed in terms of *apriori* probability $P[\alpha_i]$, as follows.

$$P[\alpha_i|e] = \frac{P[\alpha_i] \prod_{k=1}^{K} P[e_k^j|\alpha_i]}{\sum_{h=1}^{I} (P[\alpha_h] \prod_{k=1}^{K} P[e_k^j|\alpha_h])} \tag{10}$$

From Equation 10, it is assumed that event-reports are statistically independent; i.e. the receiver node is unable to figure out dependencies in reports from different vehicles, which is rational whereas such an information is not provided within reports. Thus, $P[e_k^i|\alpha_i]$ represents the probability that k^{th} report confirms the event α_i, given that α_i occurred. By recalling Equation 9, probability and weights of reports can be equalized as:

$$P[e_k^i|\alpha_i] = F(e_k^i) \tag{11}$$

In case of detecting, a further report that does not confirm the event α_i, given that α_i occurred. It would correspond to a malicious or deceiving node, who is reporting a fake event. So, the probabilistic complement is denoted by Equation 12.

$$P[e_k^j|\alpha_i] = 1 - P[e_k^i|\alpha_i] = 1 - F(e_k^i) \quad \forall \ i \neq j \tag{12}$$

Dempster-Shafer Theory

One characteristic of DST remains in the tractability of evidence, even though there is lack of information upon reported events. By the occurrence of two clashing events, measured uncertainty about one may serve as supporting evidence for other. In comparison with BI, the probability is replaced by an uncertainty interval, upper bounded by *plausibility* and lower bounded by *belief*. The belief value assigned to an event α_i is provided by the K^{th} report as the sum of all basic belief assignments $m_k(a_q)$, where a_q collects all basic events that integrate the event α_i. Correspondingly, the plausibility value of an event α_i is the sum of all evidence that does not refute such event. Thus, *belief* and *plausibility* are described by Equations 13 and 14, respectively.

http://dx.doi.org/10.5772/55453

$$bel_k(\alpha_i) = \sum_{q:\alpha_q \subset \alpha_i} m_k(\alpha_q) \tag{13}$$

$$pls_k(\alpha_i) = \sum_{r:\alpha_r \cap \alpha_i \neq \emptyset} m_k(\alpha_r) \tag{14}$$

In regard of this, data fusion can be performed to find the merged weight d_i respect to event α_i. Indeed, it is the same belief (see Equation 15) expression, such that $pls(\alpha_i) = 1 - bel(\overline{\alpha_i})$,

$$d_i = bel(\alpha_i) = m(\alpha_i) = \bigoplus_{k=1}^{K} m_k(\alpha_i) \tag{15}$$

where each piece of evidence is blended by making use of Dempster's rule of combination, as follows:

$$m_1(\alpha_i) \bigoplus m_2(\alpha_i) = \frac{\sum_{q,r:\alpha_q \cap \alpha_r = \alpha_i} m_1(\alpha_q) m_2(\alpha_r)}{1 - \sum_{q,r:\alpha_q \cap \alpha_r = \emptyset} m_1(\alpha_q) m_2(\alpha_r)} \tag{16}$$

Summing up, Figure 5 depicts system blocks for DCTE framework.

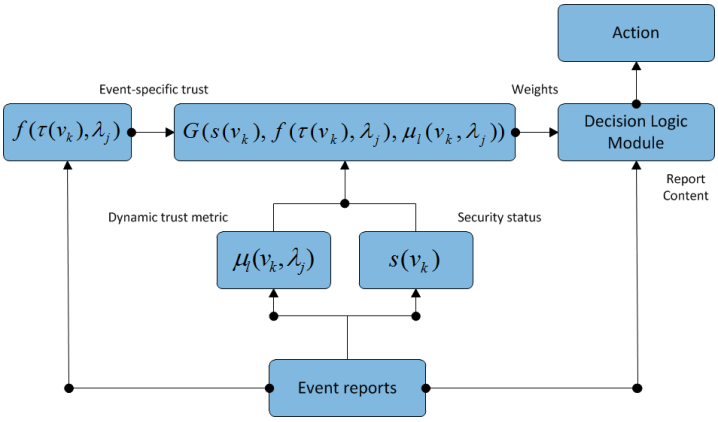

Figure 5. Data-centric Trust Establishment system blocks [21].

3.3.4. DCTE remarks

DCTE model appeals for a simple, system- and protocol-independent framework, composed basically by two stages: trustworthiness assessment and decision logic. Not only, the trust

model is mathematically described, but also the entire VANET environment. Therefore, composite variables translated into vehicles typification, event-reports, system tasks, security issues and evaluation metrics are integrally controlled by modules of general description. The intercourse of functions is based on plain operations, whilst outputs remain within unit-value intervals. Furthermore, the induction of Bayesian inference and Dempster-Shafer theory as fusion techniques offers a novel view for handling of unions and intersections of compound events. So far, CoRS and TRIP models performed either polling or weighting procedures to cope with that issue, but formal results are not sufficiently derived.

As the foregoing fellow models, DCTE delegates the authentication, integrity and confidentiality issues on exogenous mechanisms; ergo nodes identities and credentials are supposed to be distributed beforehand. And then, the exposure to security and privacy-related attacks are current concerns. Moving apart, one of the premises adopted by DCTE is the ephemeral nature of nodes' relationships in VANETs, which urges to perform trustworthiness assessment per event. The actual impact of such a situation on information sparsity needs further research.

3.4. Distributed Emergent Cooperation through Adaptive Evolution - DECADE

In [24], a game theoretic trust model is proposed, whose aim is encouraging forwarding cooperation in MANETs. The model, called DECADE, uses a non-cooperative game to achieve cooperation among rational nodes and isolation of selfish nodes. Furthermore, due to the distributed nature of the evolution algorithm and the trust evaluation mechanisms, forwarding cooperation emerges with a low overhead on computational and communication resources. Although DECADE was designed for general MANET environments, there are several elements of interest in DECADE that can be considered specifically in VANETs. So, in this section we briefly describe DECADE principles and then discuss its potential contributions to VANETs.

3.4.1. The Basic Game Model in DECADE

In transmitting a packet, every node in a path plays a role as a source, intermediate, or destination node. As an intermediate node, it has to decide whether to forward or discard a received packet based on a strategy. This strategy will depend on the trust level that the intermediate node has on the source node, and on the recent behavior of the network as a whole with its own packets. Each node is supposed to be able to observe the decisions taken by its neighbors and by all nodes preceding it in a path, so the trust on each observed node can be computed as the number of forwarding decisions among the last m observations. The limited memory, m, accounts for the fact that nodes can change their strategies continuously in order to adapt their behavior to environmental changes, so its value obeys a trade-off: m has to be large enough to obtain a fair evaluation of the forwarding rate, but m has to be small enough to ensure that the forwarding rate actually corresponds to the current strategies.

An intermediate node must be very careful to discard a packet because observing nodes can reduce their trust on it; but it cannot cooperate indiscriminately in order not to become a "sucker", wasting valuable resources forwarding packets from selfish nodes. Taking this trade-off into account, the strategy in the forwarding game is encoded by a string of bits that represents the decision of discarding or cooperating, depending on the trust level that the

http://dx.doi.org/10.5772/55453

node has in the source node, and on the number of successful transmissions within the last k own packets.

Each node participates in repeated games, where the decision to cooperate or discard of each intermediate node obeys to its current strategy. A game consists on the successful or failed transmission of a packet. Whenever a node is ready to send a packet, it chooses the most trusted path to the destination, i.e., the one that maximizes the probability that the packet gets its intended destination (which can be found through a shortest path routing algorithm under the appropriate distance metric). Then, the source node sends the packet on this path and each intermediate node decides whether to forward it or to discard it, according to its own strategies. The game ends either when the packet is delivered to its destination, or when an intermediate node decides to discard the packet. Once the game has finished, each intermediate node receives a payoff according to its decision, where forwarding decisions are paid in direct proportion to the trust level in the source node (rewarding cooperation), while discarding decisions are paid in inverse proportion (rewarding resource savings).

Given the game theoretic network trust model, it is important to find an optimal strategy for each node, so that the network as a whole maximizes both the cooperation among rational nodes and the isolation of selfish nodes. This will be done through a genetic algorithm that will evolve constantly to track the dynamical changes within the network.

3.4.2. Genetic Algorithm for Strategy Evolution

DECADE uses a distributed genetic algorithm of the cellular type with plasmid migration heuristics, which not only gives good results in term of the optimality of the converged solutions, but also exhibits good adaptability to changing conditions. Each node tries to maximize its payoff by exchanging periodically genetic information with its neighbors in order to evolve the strategy. As in a classical cellular genetic algorithm, each node receives the genetic information from all its one-hop neighbors, selects randomly two of them with a probability of being selected proportional to their fitness and, through the classical one point cross-over and mutation processes, combines them to construct a new strategy. This classical cellular mechanism is enhanced with a bacterial plasmid migration concept, where two heuristics are added. First, each node can accept or reject the new strategy depending on whether the reported fitness is greater or smaller than its own fitness. Second, each node can keep a copy of its best previous strategy so that, if during the current plasmid migration period the new strategy did not increase the fitness, the old strategy can be restored. An important heuristic in this evolution process is that, since each node keeps a record of its best strategy so far (plasmid genes instead of chromosomal genes), a node can replace the current strategy with the stored one, just before any strategy exchange among neighbors takes place. This heuristic enhances the exploratory capacity of the evolution process.

3.4.3. DECADE remarks

Intended to encourage forwarding cooperation in MANETs, DECADE achieves remarkable performance results in cooperation among rational nodes, isolation of selfish nodes and adaptability to changing environments. Furthermore, due to the distributed nature of the evolution algorithm and the trust evaluation mechanisms, cooperation emerges with a low overhead on computational and communication resources. However, although forwarding decisions could become an issue in some infotainment applications of vehicular ad hoc

networks, the most important current problem in VANETs is in content trust and reputation, not addressed by DECADE. We just mentioned DECADE because it points out to the potential of complex systems engineering for trust and reputation systems in VANETs. Indeed, the whole system develops the cooperation as an emergent phenomenon, which appears as a consequence of individual decisions, based on local observations. Each node wants to save its scarce resources by using them rationally, seeking the cooperation of intermediate nodes to deliver their own packets. As a consequence of the local interactions among nodes, the global cooperative behavior arises, with the reported performance benefits. This approach should be explored more extensively in the engineering of VANET systems.

4. Trust and reputation model comparison

In regard of the foregoing trust and reputation passage, including general specifications, design criteria and structured mechanisms, we conclude the present chapter with an overall analytical comparison upon the studied models. Firstly, Table 3 gathers the capabilities of CoRS, TRIP, DCTE and DECADE with respect to the models' considerations, as a matter of design, implementation and support. Please note, three possible qualifications (T=Total, P=Partial, F=Fail) can be given in order to reflect their strengths and downsides.

Criterion	CoRS	TRIP	DCTE	DECADE
Low Complexity	P	P	T	T
Scalability	T	T	T	P
Sparsity	T	P	P	P
Security and privacy-related	T	P	P	P
Mobility patterns independent	P	P	P	P
Trust and reputation decentralization	P	P	T	T
Confidence measure	F	T	T	P
Event and spatiotemporal specification	T	T	T	T

Table 3. Criteria comparison among trust and reputation models.

Closing up, the qualification chart onto *low complexity* criterion. CoRS and TRIP protocols incorporates multi-purpose modules to improve the efficiency on trustworthiness computation, messages convergence, resilience and others. However, the employment of those metrics moving upward the protocol's performance, also impacts noxiously the altogether complexity levels. Likewise, *trust and reputation decentralization* criterion is partially fulfilled by CoRS and TRIP protocol, while DCTE and DECADE achieves a "Total" mark. One more time, the model conceptualization is intrinsically related to third-party entities, which are set up to enhance particular aspects in security matters. Indeed, DCTE and DECADE are also pending to explain how the confidentiality, integrity and authentication issues are natively handled. In the meantime, the top score is granted, assuming the engagement of exogenous mechanisms.

A limited performance seems to be equally exhibited by all the examined protocols with respect to *sparsity*. Taking CoRS out of this group; the introduction of cryptographic thresholds boosts the dissemination of information sources, according to the scarcity conditions on the road. From the bulky generation of shares, the model previously knows

http://dx.doi.org/10.5772/55453

the actual capabilities of the mobile nodes to interact among them. Then, scenarios with lack of resources can be foreseen based on some degree of certainty. On the contrary, the remaining models do not follow a self-sustained strategy to adapt their mechanisms to selective information retrieval. However, potential potential bases are grounded to achieve flexible thresholds on trust and reputation assessment. For instance, TRIP and its fuzzy set of rules might be easily extended to actively manage to this requirement. A quite similar diagnosis can be emitted about *mobility patterns independent* criterion, where every protocol is marked as "Partial". Notwithstanding, the assurance of a "Total" mark on this concept would require a massive set of tests, regarding simulated and real scenarios. Until now, the achievement of common levels of agreement on this matter are very unlikely.

Outstandingly, *scalability* and *event and spatiotemporal specification* criteria are satisfactorily attained by the group of models. The former one can be possibly explained by the accelerated development of powerful processing platforms, whose physical resources are capable to adjust to the ongoing demands, neatly. In turn, replaying to what, when and where issues regarding the events on the road shall be imposed as a compulsory requirement for a trust and reputation model. Otherwise, practical usages of such protocols could be easily questioned.

Furthermore, trustworthiness computation metric is definitively one of the most interesting aspects to be differentiated in each trust and reputation model. Therefore, it is worthwhile to take a quick tour around the employed assessment techniques. Considering CoRS protocol, *majority voting* stands out as the selected method to obtain the trust level TL upon a particular event. Thus, Equation 17 depicts the value computed by K nodes, where each one contributes with a +1 reward for a confirmed on road event α_i. Likewise, negative or neutral values may apply in case of fake or deceiving information.

$$TL = \frac{1}{K} \sum_{k=1}^{K} f(\alpha_i) \tag{17}$$

In respect to TRIP protocol, *weighted polling* acts as the calculation method for trustworthiness modeling. Thereafter, all given recommendations or reports about an event $f(\alpha_i)$ is affected by an scalar weight w, whose value takes into consideration information sources, penalties and rewards history, VANET complexity, etc. The trust level TL performed by TRIP mode follows the general rule in Equation 18.

$$TL = \frac{1}{K} \sum_{k=1}^{K} w * f(\alpha_i) \tag{18}$$

For DCTE framework, a couple of data fusion techniques are designated for trust and reputation measurement. In section 3.3.2, we have introduced Bayesian inference as a statistical approach and Dempster-Shafer theory for evidence evaluation inspired in human reasoning. For the implicit mathematical description refer to the corresponding section.

5. Conclusions

Vehicular Ad Hoc Networks constitute an emergent and fascinating research field.Many conceptual architectures, abstract models and heuristic-derived systems are continuously proposed to cope with the many issues that arise in this area. In this chapter we have made an effort to describe four of the most remarkable approaches in literature.

CoRS model implements threshold cryptography in a distributed way, achieving low complexity in security management. In fact, CoRS might be considered one of the most efficient and effective protocols, although special attention should be given to crowded networks, since the distribution of repeated shares might lead to system's collapse. Similarly, the collator player is a potential faulty point because it is the only party designated to set time and location of events.

A strength of the TRIP protocol is the use of multiple information sources like direct peers, referred nodes and central entities. Also the well-defined system of penalties and rewards makes of TRIP a robust framework for trust and reputation determination. A differentiator factor of TRIP is its support of trust and reputation scoring system on adaptable probabilistic functions. However, TRIP has some reliability difficulties to solve.

DCTE strives to deal with trustworthiness assessment, decision logic and environment description. These aspects are integrated through fusion techniques, generating representations of trust and reputation scores that achieve both simplicity and efficiency. Unfortunately, DCTE has major issues in confidentiality, authentication and integrity aspects, which are assumed to be carried out by third party schemes.

We also introduced DECADE as a newcomer model, given its good performance within MANETs. The protocol encourages cooperation among rational nodes, isolating selfish nodes with high adaptability to changing environments. Useful concepts such as the emergence of a cooperative behavior from simple individual decisions based on local observations, with very low overhead, points out at the convenience of facing trust and reputation mechanisms in VANETs through the theory of complex systems. Although DECADE only addresses the MANET problem of node trust and reputation, its emergent approach could be used in the most urgent VANET problem of content trust and reputation.

Finally, considering eight criteria (complexity, scalability, sparsity, security, mobility dependence, decentralization, confidence measure and event specification), we compare the four selected approaches and notice that none of them satisfy all the criteria. However, with the exception of independence on mobility, all the different criteria are satisfied but at least one approach. A good research line would be to exploit the advantages of each proposal looking for a general framework where to put over solid basis the development of Distributed Trust and Reputation Mechanisms for Vehicular Ad-hoc Networks.

Author details

Marcela Mejia[1] and Ramiro Chaparro-Vargas[2]

1 Universidad Militar Nueva Granada, Bogotá, Colombia
2 RMIT University, Melbourne, Australia

http://dx.doi.org/10.5772/55453

References

[1] M. Gerlach and F. Friederici. Implementing trusted vehicular communications. In *Vehicular Technology Conference, 2009. VTC Spring 2009. IEEE 69th*, pages 1 –2, april 2009.

[2] P. Papadimitratos, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger, M. Raya, Zhendong Ma, F. Kargl, A. Kung, and J.-P. Hubaux. Secure vehicular communication systems: design and architecture. *Communications Magazine, IEEE*, 46(11):100 –109, november 2008.

[3] P. Ardelean and P. Papadimitratos. Secure and privacy-enhancing vehicular communication: Demonstration of implementation and operation. In *Vehicular Technology Conference, 2008. VTC 2008-Fall. IEEE 68th*, pages 1 –2, sept. 2008.

[4] J. P. Hubaux P. Papadimitratos, V. Gligor. Securing vehicular communications - assumptions, requirements, and principles. november 2006.

[5] F. Kargl, P. Papadimitratos, L. Buttyan, M. Muter, E. Schoch, B. Wiedersheim, Ta-Vinh Thong, G. Calandriello, A. Held, A. Kung, and J.-P. Hubaux. Secure vehicular communication systems: implementation, performance, and research challenges. *Communications Magazine, IEEE*, 46(11):110 –118, november 2008.

[6] M. Raya, P. Papadimitratos, and J.-P. Hubaux. Securing vehicular communications. *Wireless Communications, IEEE*, 13(5):8 –15, october 2006.

[7] P. Papadimitratos, L. Buttyan, J. P. Hubaux, F. Kargla, A. Kung, and M. Raya. Architecture for secure and private vehicular communications. 2007.

[8] T. Leinmüller, L. Buttyan, J. P. Hubaux, F. Kargl, R. Kroh, P. Papadimitratos, M. Raya, and E. Schoch. Sevecom - secure vehicle communication. june 2006.

[9] L. Buttyan and J. P. Hubaux. Security and Cooperation in Wireless Networks. http://secowinet.epfl.ch, 2007. Cambridge University Press.

[10] P. Papadimitratos and J. P. Hubaux. Report on the secure vehicular communications: Results and challenges ahead workshop. april 2008.

[11] D. Djenouri, W. Soualhi, and E. Nekka. Vanet's mobility models and overtaking: An overview. In *Information and Communication Technologies: From Theory to Applications, 2008. ICTTA 2008. 3rd International Conference on*, pages 1 –6, april 2008.

[12] Félix Gómez Mármol and Gregorio Martínez Pérez. Trip, a trust and reputation infrastructure-based proposal for vehicular ad hoc networks. *Journal of Network and Computer Applications*, 35(3):934 – 941, 2012. <ce:title>Special Issue on Trusted Computing and Communications</ce:title>.

[13] Jie Zhang. A survey on trust management for vanets. In *Advanced Information Networking and Applications (AINA), 2011 IEEE International Conference on*, pages 105 –112, march 2011.

[14] A. Tajeddine, A. Kayssi, and A. Chehab. A privacy-preserving trust model for vanets. In *Computer and Information Technology (CIT), 2010 IEEE 10th International Conference on*, pages 832 –837, 29 2010-july 1 2010.

[15] R. A. Chaparro-Vargas. A security infrastructure for an in-vehicle middleware based on device profile for web services. M.sc. thesis, Munich, 2010.

[16] Marcela Mejia, Néstor Peña, José L. Muñoz, Oscar Esparza, and Marco A. Alzate. A game theoretic trust model for on-line distributed evolution of cooperation in manets. *Journal of Network and Computer Applications*, 34(1):39 – 51, 2011.

[17] C. S. Eichler. *Solutions for Scalable Communication and System Security in Vehicular Network Architectures*. Dissertation, Technische Universität München, Munich, 2009.

[18] Aifeng Wu, Jianqing Ma, and Shiyong Zhang. Rate: A rsu-aided scheme for data-centric trust establishment in vanets. In *Wireless Communications, Networking and Mobile Computing (WiCOM), 2011 7th International Conference on*, pages 1 –6, sept. 2011.

[19] Adi Shamir. How to share a secret. *Communications of the ACM*, 22(11):612–613, november 1979.

[20] Anand Patwardhan, Anupam Joshi, Tim Finin, and Yelena Yesha. A data intensive reputation management scheme for vehicular ad hoc networks. In *Mobile and Ubiquitous Systems - Workshops, 2006. 3rd Annual International Conference on*, pages 1 –8, july 2006.

[21] M. Raya, P. Papadimitratos, V.D. Gligor, and J.-P. Hubaux. On data-centric trust establishment in ephemeral ad hoc networks. In *INFOCOM 2008. The 27th Conference on Computer Communications. IEEE*, pages 1238 –1246, april 2008.

[22] Qing Ding, Xi Li, Ming Jiang, and XueHai Zhou. Reputation-based trust model in vehicular ad hoc networks. In *Wireless Communications and Signal Processing (WCSP), 2010 International Conference on*, pages 1 –6, oct. 2010.

[23] N.-W. Lo and Tsai H.-C. A reputation system for traffic safety event on vehicular ad hoc networks. page 10, 2009.

[24] Marcela Mejia, Néstor Peña, José L. Muñoz, Oscar Esparza, and Marco Alzate. Decade: Distributed emergent cooperation through adaptive evolution in mobile ad hoc networks. *Ad Hoc Networks*, 10(7):1379 – 1398, 2012.