SURVEY ON SECURE ROUTING IN VANETS

Afef Slama[1] and Ilhem Lengliz[2]

[1]HANA Laboratory, University of Manouba, Tunisia
[2]Computer Science Department, Military Academy, Tunisia

ABSTRACT

Vehicular Ad Hoc Networks (VANETs) are based on network technology where cars act as mobile nodes to form a communication network. In VANETs, routing protocols have a significance regarding the overall network performance since they determine the way of sending and receiving packets between mobile nodes. Most of the protocols proposed for VANETs are adapted from Mobile ad hoc networks (MANETs) routing protocols. However, due to the specific characteristics of VANETs, especially high mobility, and dynamic topology, the routing protocols in ad hoc networks do not adapt immediately to VANETs. Therefore, secure routing of Vehicular ad hoc networks (VANETs) against attacks, which are of various types, is still a challenging issue. This paper is going to present a synthesis of the most relevant protocols that have addressed the secure routing issue in VANETs. It also establishes a comparison regarding the offered features and the studied performance aspects through which it is notified that a security mechanism depends not only on the level of efficiency but also on the network constraints.

KEYWORDS

VANET, routing, secure routing, attacks & performance

1. INTRODUCTION

The unique characteristics of VANETs, such as network topology, high mobility, and frequent topology variations, and density of vehicles, raise particular challenges for the design of any routing process. In effect, the network features may affect the routing strategy in terms of routing protocols inadequacy. Thus, an efficient routing protocol design for VANETs is extremely important.

The main security aims (authentication, integrity and potential non-repudiation) are suitable for the potential needs of secure VANET routing [1]. Since the security and the privacy of the nodes are of major importance, the verification of the routing messages is a big challenge in VANETs [2-3]. Indeed, each vehicle is required to check the authenticity of any received routing message, thus making sure that it was sent from an authentic vehicle. Secure routing guarantees that the intermediate nodes in multi-hop forwarding data packets have neither dropped the packets nor just modified their contents.

Besides, most VANETs applications require secure routing, mainly vehicle safety applications, which are among the major drivers for VANETs as they affect people's lives [4]. In the last few years, more accident cases have been identified; consequently, the growing problem of accident and traffic jam legitimates the adoption of Intelligent Transportation Systems [5-6]. Although cellular networks enable convenient communication both for drivers and passengers, they are not suitable for the vehicular environment, especially with regard to enhancing safety. VANETs provide direct communication between vehicles, and to/from Road Side Units (RSUs). Hence, during the data switching process, receiving and sending dangerous warnings and information

about current traffic situations can be made with minimum latency. Exchanging such warning messages which aim to avoid accidents would increase passengers' safety between vehicles, involving relieving over crowdedness and boosting operation management for public safety. Indeed, VANET communications are meant to pre-alert the driver as well as the vehicle through a stretched information horizon in case of any possible hazardous states, in order to improve people's life quality [7]. It turns out that working on the securing of the routing protocol deployed in a VANET can help with an in-depth address of this issue.

The oncoming part of this paper is organized as follows: In section 2, VANETs attacks are reviewed, along with the related secure mechanisms. Section 3 provides a summary of existing proposals for secured routing in VANETs. In section 4, a comparison of the surveyed protocols is elaborated. Section 5 discusses the challenges to address when designing secure routing protocols. Finally, the conclusion is drawn in section 6.

2. VANETS ATTACKS AND RELATED SECURITY MECHANISMS

In Intelligent Transportation System (ITS), each vehicle plays the role of a transmitter, an addressee or a router to send information to the vehicular network or to the transportation agency which then uses the received information to ensure safe, free flow of traffic [8-9-10]. Unfortunately, this information can be altered due to malicious nodes. Thus, it is necessary to secure the routing messages against various attacks [11]. As a result, a synthesis of those attacks is presented in this section besides the related security mechanisms.

2.1. VANETS ATTACKS

2.1.1. Attacks on Availability

Availability means that any information must be available at any time of the communication process. Availability in a VANET should be assured both on the communication channel and within the participating nodes [12]. These attacks are classified as follows:

- Black Hole Attack: in this attack, the attacker node can drop the packet or decline to participate in the routing process.
- Malware: it is malignant software held by an insider, whose purpose is to disturb the normal network operation.
- Broadcast Tampering: in this type of attack, the attacker inserts a false safety message into the network.
- Spamming: spamming is the irrelevant or unsolicited messages sent over the Internet, like advertising.
- Greedy Drivers: they are those individuals who aim to attack for their own profit.
- Denial of Service: here, the attacker crams the most important communication medium. The main objective is to prevent legitimate users from accessing the network services and from using network resources [2].

2.1.2 Attacks On Authentication /Identification

Basically, authentication is a process necessary for every vehicle before accessing a VANET and utilizing its resources [13]. Thus, the identification code is a basic requirement to meet so that only a trustworthy sender vehicle can be allowed to communicate with others. Therefore, authentication can be considered to be the first line of defense against intruders [2]. The attacks related to authentication are:

- Masquerading: in this type of attack, an attacker gives a false identity using the communication process.
- Replay Attack: it occurs when an attacker reproduces the transmission of previous information to take advantage of the state of the message at the sending time [12].
- Global Positioning System (GPS) Spoofing: in this attack, an attacker provides false information by bringing in false readings in GPS devices.
- Tunneling: an attacker can lead an analysis of traffic or a selective forwarding when two distant nodes use an extra communication channel as a tunnel.
- Sybil Attack: the attacker asserts they have many identities to force other vehicles to go away from the road for their own benefit.
- Message Tampering: an attacker pretends to modify, to drop or to corrupt an important or even critical traffic safety message.
- ID Disclosure: in this type of attack, the ID of targeted nodes will get disclosed for tracking the present position of that node by sending malicious code to the neighbors [2]. A globular viewer controls the target nodes and can even send a malicious message to the neighbor of targeted nodes [12].

Thus, the lack of adequate authentication mechanisms could have a detrimental impact on the whole security of the VANET [7].

2.1.3. Attacks On Confidentiality

The secret aspect of messages exchanged between the nodes of a vehicular network is especially weak in comparison to techniques like the illegitimate collecting of messages through eavesdropping and the accumulation of location-related information available through the transmission of broadcast messages [8]. In the case of eavesdropping, the assailant can gather and make use of information about drivers without their authorization. That is why the data must be untouched during the routing process until they reach the destination [2].

2.1.4. Attacks on Privacy

In this type of attack, an attacker aims to illegally access some information about vehicles. Because of the direct relationship between a driver and his/her vehicle, the attacker can act on the driver's privacy by means of identity revelation or location tracking. Therefore, robust privacy preservation techniques are required to reassure the users and invite them to disclose their exact position [7].

2.1.5. Attacks Non-Repudiation

Each user must be distinguished from others so that the users' actions cannot be repudiated. Non-repudiation aims to avoid one entity denying having done some action [2]. Thus, the same key in various vehicles should be obviating by using secure storage.

2.1.6. Attacks on Data Trust

Data trust is defined as the assessment of whether or not and to what extent the reported traffic data are trustworthy [4]. Data trust may be endangered by incorrect data computation or by transmitting affected messages. This can be done by handling sensors in the vehicle or by altering the transmitted information.

2.2. SECURITY MECHANISMS

Given the diversity of the possible threats and attacks on VANETs, each vehicle must be capable of assessing, of making a decision and of locally reacting on information obtained from other vehicles based on security mechanisms [14]. To this end, existing security solutions are typically divided into two main categories: cryptography and trust [15].

The first category is cryptography. It is the practice and study of techniques for secure communication in the presence of adversaries [16]. Cryptography uses methods and processes such as encryption/decryption algorithms, keys generation, and exchange protocols, hash functions and digital signature [17]. The most relevant cryptography methods are symmetric and asymmetric cryptography. Asymmetric cryptography is also called secret key or private key cryptography. This key should be shared between the sender and the receiver before secure message exchanging [18]. Both sender and receiver share only one key to encrypt and decrypt the messages. As far as asymmetric cryptography is concerned, it is known as public key cryptography. This method uses two keys: a public key and a private one [18]. Each user must keep secret his/her private key while making available their public one. When a message is encrypted with the public key, it can be decrypted only with the private one. It is practically impossible to determine which private key knows the public one and vice versa [17]. The management of private and public keys for a large number of users requires the establishment of a PKI: Public Key Infrastructure, which is a set of software, hardware and procedural components [17]. Thus, a Certification Authority (CA) will be responsible for generating and managing digital certificates. Each CA would be responsible for a specific area, for instance, a national zone, a district or a town. It's the duty of these authorities to assume and tackle the credentials and identities of all the vehicles registered under their hood [19].

The second category is called trust. It appeared as a complement to cryptography on some specific adversary models and environments where the latter were not enough to mitigate all possible attacks. A number of trust-based methods have been proposed to achieve security in VANETs such as plausibility based on sensor-driven techniques and reputation systems. Indeed, a secure system should be able to recognize faults in a sensitive and a fast way. This is realized by the plausibility checks on the exchanged routing control messages among vehicles [20]. Plausibility checks can be applied as part of an in-depth defense concept to prevent attacks on safety critical functions [21]. They can be performed by comparing the message obtained from all the other nodes with the state of the neighboring environment provided by sensors or by pre-designed models, given that reputation systems are programs that allow users to rate each other in online communities in order to build trust after some verification or prior interaction [22]. The underlying idea of reputation systems is that even if the node cannot verify the reliability of source information, it still can be confident in the content of the exchange through trust built by recommender systems. Hence, trust management was mainly conceived to decide whether to believe or disbelieve information asserted by other nodes [15].

3. SECURE ROUTING PROTOCOLS FOR VANETS

A lot of effort has been put into research in the area that focuses on establishing security in VANETs. For the purpose of this survey, the most recent security techniques proposed for VANETs are analyzed below. As they can be used in the design of a VANET secure routing protocol. In fact, these security techniques do include routing packet exchanges and transfer. Indeed, any security technique proposed for data packet transfer can be adapted to the specific routing packet transfer.

3.1. CRYPTOGRAPHY-BASED PROTOCOLS

3.1.1. SEPPBR

Hou and al. [23] have proposed a Secure and Efficient Protocol for Position-based Routing in VANETs (SEPPBR) that acts by means of two mechanisms. The first mechanism is based on routing message protection. A signature -checking plan is used in order to fulfill end-to-end and hop-to-hop authentic and integrated data. The authors added a signature field to the structure of the GPSR (Greedy Perimeter Stateless Routing) data packet. They assume that every node has an ID-based private key (keyPri) and a public key (keyPub). The sender calculates the signature based on keyPri and a hash function before sending a packet. Then, the receiver of the routing data packet checks it using keyPub. The second mechanism is divided into two aspects: a forward and backward evaluation. Forward evaluation is used to determine the drop-malicious nodes. Packets forwarded by wormhole malicious node will be considered to be a dropped packet. Then the routing scheme will change the transmit path. Backward evaluation is used to detect the tamper-malicious nodes. The sender is assessed by the receiver in order to drop the tampered packets. Each node operates through a hybrid surveillance mode and verifies each packet received by its neighbor. The protocol evaluation of neighbor nodes reliability is stated by verifying its forwarding ratio (the ratio of packets forwarded to received ones).

The main contribution of this solution is that the problem which the cryptosystem cannot tackle, such as dropping packets to ruin the efficiency of the routing protocol, has been solved.

3.1.2. EMAP

VANETs take up a PKI and Certificate Revocation Lists (CRL) to secure data. Each CRL holds the rescinded certificates declared by the CA. Thus, the authenticity of each received message must be firstly verified by checking the revocation status of the sender in the CRLs before checking the sender's certificate and the sender's signature in a PKI system. Hence, checking the revocation status of the emitter takes a huge amount of time. It depends on the CRL size and the techniques used to examine the CRLs. The CRL size rises greatly since all OBUs are preloaded with nameless digital certificates (CERTu) which must be frequently replaced. Indeed, EMAP, which stands for Expedite Message Authentication Protocol for Vehicular Ad Hoc Networks, was proposed [24] to fix this problem. For this purpose, it substitutes the time-consuming CRL checking process by an effective revocation verifying process. Before broadcasting a message, each OBU calculates its revocation check (REVcheck). This revocation check process uses a keyed-Hash Message Authentication Code (HMAC), where the key used in calculating the HMAC is shared only between non-revoked OBUs. This secret key is denoted Kg. Each message must be sent to its REVcheck which will be compared with the value determined by the receiver's OBU. In the case of non-equality, the certificate of the OBU is revoked by the CA and a new secret key Kg is broadcasted to all the non-revoked OBUs. EMAP uses a new probabilistic key distribution method which allows non-revoked OBUs to securely partake and update the secret key securely.

3.1.3. AMLA

AMLA [25] is a novel protocol for Authentication with Multiple Levels of Anonymity. This protocol makes use of an identity-based signature mechanism along with pseudonyms to implement anonymous authentication with a non-repudiation and integrity source. Each vehicle is fitted with a set of pseudonyms. The number and the lifetime of each pseudonym lean on vehicle anonymity requirements. Then, reviewing only a limited group of pseudonyms is satisfactory to engender a unique and a particular different pseudonym. Besides, this protocol cryptographically binds an expiry date to each pseudonym, and in this way enforces an implicit

revocation for the pseudonyms without the use of any public key certificates. In AMLA, radio towers are supposed to be connected to a server machine called Security Service Provider (SSP) and each vehicle is equipped with a TPD which contains the secret keys. Those secret keys are appraised or revised only with the private key generator SSP. This protocol operates with Identity-Based Encryption (IBE) and the signature mechanism. Thus, a sender transmits a message signed by a private key conform to one of its pseudonyms (PrX) stored in the Pseudonym Database (PDB). The receiver of a message extracts PrX from the message and checks its validity in the Data Issuance Table (DIT) which stores only pseudonyms issued in the current date. In case of validity, the public key of the sender (PIKrx) is extracted using a Hash function, and the digital signature packed with the message is verified using the public key of the SSP (SSPpub). In the opposite case, the expired pseudonym must be renewed when the vehicle is not compromised. For this purpose, the SSP initiates a new unique pseudonym with the same lifetime, brings about the correlating private key and updates both the PDB and the DIT.

3.1.4. S-BRAVE

Secure-Beacon-less Routing Algorithm for Vehicular Environments (S-BRAVE) [26] was developed as an extension to the Beacon-less Routing Algorithm for Vehicular Environments (BRAVE). S-BRAVE addresses the security menaces related to Position-Based Routing (PBR) protocols [27]. In S-BRAVE, messages are signed by taking advantage of PKI. Hence, the emitter uses its private key to sign data packets. Then, the receiver must use the public key of the transmitter included in the digital certificate to verify the validity of the data. The certificate is generated by a unique trusted CA for all the vehicles. In BRAVE, the certificate is not included in every message. However, a cache of known neighbors is included in each beacon transmitted. Every vehicle whose certificate is stored inside is acknowledged as a neighbor. In this way, the number of certificates exchanged is reduced. S-BRAVE is based on the same certificate exchange scheme with some modifications. It adds the concept of watchdog or guard node. Indeed, every neighbor in front of the vehicle will behave as a guard node. The Guard node keeps listening to the next forwarder, thus verifying if it retransmits the data message. If the selected node does not forward the packet, the neighboring node plays the part of the next forwarder by assuming the responsibility of sending the data message to the next hop. The guard node also includes the detected malicious node in a blacklist for fear that it might get selected as the next forwarder in the future. The sender initiates a DATA packet and waits for responses. Then, if that vehicle is the destination, the vehicle that receives the DATA message answers with a RESPONSE and schedules a timer to receive the SELECT message. In the reverse case, only the nodes that afford routes to the destination will give a RESPONSE after a certain time. Therefore, a SELECT message is sent to the most promising forwarder. In the case of non response, the guard node becomes the current forwarder and the vehicle is added to a CRL. This process will continue until it reaches the previous hop that allows the selected forwarder to deliver an ACK.

3.2. TRUST-BASED PROTOCOLS

3.2.1. MHLVP

Multi-hop Location Verification Protocol (MHLVP) [28] was launched in order to check on the inquired vehicle and its announced location using a cooperative multi-hop approach whenever forward checking and communication are impossible. Since obstacles affect the integrity and reliability of localization services, it is imperative to overcome their effects on communication transmissions. These obstacles such as buildings could block vehicles serving as neighbors in the same communication range. The offered solution raises neighbors' consciousness and

vehicles' observation towards the nodes enclosed under non line of sight conditions. Every vehicle is apt to determine its own location using a technology such as GPS. It checks direct neighbors and measures the emitter's corresponding distance in order to store it in a database. This table is then updated following the mobility of the nodes. Let us take a node A which wants to communicate with a node C in presence of an obstacle between the two nodes and let us suppose that a node B has a direct communication with both A and C. Node A broadcasts a request to its direct neighbors to find a way to reach node C. The receiver of the request verifies the existence of the sender in the neighborhood list and rebroadcasts the demand until a node with a direct communication with the destination C is found. Then, triangular calculations are used to determine the C's location and the distance dc using the node B. Consequently, the intermediate node sends a reply message containing the distance and the number of hops to reach the destination. The sender will receive responses from different nodes and must be able to select the one that matches information stored in the database. The request must be abandoned in case of no reply or after its lifetime to eliminate false data has expired.

3.2.2. DAATM

Gazdar and al. [29] proposed a distributed advanced analytical trust model for VANETs (DAATM). It blends the entity and the data-oriented approaches. This dynamic model establishes the immediate supervision of the vehicle behaviors in the network in order to remove malignant nodes. Thus, every vehicle is able to fulfill an autonomous trust metric appraisal based on the previously occurring messages. If an event appears in the network, alert messages are forwarded by each vehicle in the neighborhood. Besides, the proposal checks the information itself to reveal its reliability. In this way, each vehicle called “monitor” changes the trust metric Tm of every vehicle called “monitored” situated in its vicinity. The assessment of the demeanor of the monitored vehicle, by the monitor vehicle is in regard to two particular facets. The first is the trustworthiness of the message addressed by the monitored vehicle and the second is its collaboration rate. Hence, Tm of the monitored vehicle must be updated by the monitor according to its behavior. The updating process uses a Markov chain with (N+1) state. For each state of the monitored vehicle a Tm value which varies in the interval [0, 1] is accredited by the monitor. State 0 is the mistrust state where Tm=0 and state N is the best-trusted state. Therefore, if a vehicle displays an acceptable behavior, its Tm is transported to the next state; otherwise, it transmits back to the previous state. The credence of the behavior refers to the capacity of the vehicle to perfectly lead all appropriate received messages, and to the lawfulness of its transmitted messages.

3.2.3. TM-AODV

Chinnaswamy and al. [30] propose a Trust Model integrated to the AODV protocol (TM-AODV). The main goal of this trust model is to identify sinkhole nodes and to avoid selecting them in the route selection phase. In this proposal, the source node broadcasts a route request (RREQ) to all nodes in its vicinity. Then, each neighbor rebroadcasts the RREQ to other nodes in the proximity until it reaches the destination. The source waits until it gets a route reply (RREP) from all the neighbors to select a route between the source and the destination. Thus, the route is not chosen in view of the first return of RREP. The selected route is the shortest one. The routing algorithm needs to react rapidly to topological changes according to the rate of trust of a node or a thorough way between the emitter and the receiver. If a link breaks during the transmission phase, a route error message is delivered and propagated back to the source which will stop its sending process and reinitiate an RREQ in order to select another route. Hence, the objective is to provide nodes with a mechanism to adjudge the trust level of its direct neighbors. This approach also uses a variation between neighbors to induce the existence of a sinkhole node. When the source receives more than one RREP providing different paths with the same

length, the model allows selecting the path with the minimum number of hops and considers others containing sinkhole nodes. Therefore, the security of the existing AODV protocol is improved by enhancing a trust-based route selection.

3.2.4. VSRP

VSRP is a Vehicular Security through Reputation and Plausibility Checks is a technique proposed by Dhurandher and al. in [31]. The suggested algorithm builds security in VANET through the exploitation of trust levels for nodes in the network based on reputation and plausibility checks. Whenever a vehicle needs to transmit an event which is sensed through its own sensors or is transmitted by a trusted vehicle, it begins a neighbor discovery phase. When a node broadcasts a neighbor request (neighbores), each receiver checks the value attributed to the sender, in its trust table. The request packet is accepted only if the node is either not in the trust table or is present with a trust value not equal to 0. Once a node has identified its neighbors, it broadcasts the data packet and inserts this event in its event table to keep a record of the fact that this event has been dispatched. When a node receives a data packet, it makes a decision and updates trust tables. If the packet is received from outside the threshold range, the packet must be dropped. Otherwise, if the event is not in the detection range of the receiver, the trust value of the sender decreases and the receiving node starts a timer and collects the responses from the other nodes. If the number of responses exceeds the threshold, the event is considered genuine and the trust values of all the sending nodes are incremented. Or else, the receiving node increases its detection range to the maximum in order to collect the responses from the other nodes. Indeed, the neighbors are monitored. Each node is able to identify whether the data are received from a malicious node or not, based on the information that is available with the node and the information that it receives. The algorithm sequesters malicious nodes.

3.2.5. DRS

Oluoch proposed a Distributed Reputation Scheme for situation awareness in VANETs (DRS) [22]. This proposal is a reputation model that helps vehicles circulating in the roads to appraise the dependableness of their associate. To bring about trust between vehicles, the receiver of a message must demand the judgment of other vehicles in its communication range. Moreover, it accumulates all assessments from the members of the group to calculate the average score in order to compare it with the threshold that was settled. Then, the reputation scores of neighbors must be stored in an array list based on their behaviors. This list is brought up-to-date after a period of time. The trustworthiness of each vehicle is a value of the interval [0, 1] where 0 is the worst trust level and 1 is the best one. This algorithm considers that a malevolent node to be the one having a reputation score inferior or equal to 5. Thereby, the reputation score of a legitimate vehicle will rise but in regard to the illegitimate ones, their tally will decrease. Also, CA cancels the dishonest vehicle's certificate. If no assessment is given by the neighborhood, the vehicle checks the opinion of the RSU. As RSU gets numerous descriptions about the roadway status, RSU is able to check the efficiency of the messages.

3.2.6. EDTCP

EDTCP is an Enhanced Distributed Trust Computing Protocol for VANETs proposed by Gazdar and al. in [32]. EDTCP is a new distributed trust computing framework based on the investigation of the direct experience between neighboring vehicles without using any recommendation system. This proposal consisted of a new tier-based message dissemination technique whose function is to efficiently detect eavesdropped messages and fake events. This protocol is based on a set of event generators randomly dispersed within the network. Alert messages are triggered in zone ZO upon the direct detection/sensing of an event, and then they

are progressively relayed throughout zone ZD. To this end, the dissemination is organized into tiers. Hence, the detection zone ZD is divided into tiers. When an event occurs on the road, a binary authentication value denoted by e.auth is assigned to this event. If the event is observed/detected by all vehicles (malicious and non-malicious) in the vicinity, e.auth equals 1 and the event is considered authentic. Otherwise, if it is only served/detected by malicious vehicles, e.auth equals 0 and the event is deemed fictitious. Before transmitting the alert message, every vehicle adds an authenticity value of the event denoted Av(e) depending on its behavior. If the vehicle is malicious Av(e) is set to 0, else it is set to 1. The processing of alert messages primarily depends on the position of the receiving vehicle called "monitor M" and on the transmitting vehicle called "monitored M". The decision made by Monitored M depends on its current tier: M is in the zone, M is in the first tier or M is in tier(M)>1. This technique guarantees that there are no possible collisions between alerts coming from different tiers about the same event, given that no two nodes from the three consecutive tiers transmit simultaneously. Based on the dissemination technique, the trust metric (Tm) of each vehicle is computed and updated by the monitor after receiving an alert message. TM is a value in [0, 1], initialized to 0.5, incremented when the vehicle transmits an authentic alert about an authentic event or decremented with a step ξ in other cases. Hence, when Tm=0, the vehicle is considered malicious.

3.2.7. CSRP-TDA

Tolba proposed a Trust-Based Distributed Authentication (TDA) method that relies on a global trust server and a vehicle behavior for avoiding collision attacks [33]. This method grounds both inter-vehicular and intra-vehicular communication security in the network. In addition, a Channel State Routing Protocol (CSRP) is proposed to improve communication reliability among the vehicles. Reliable vehicles are identified according to the onboard unit (OBU) energy and the channel state of the vehicle in terms of delivering seamless communication. The CSRP minimizes the energy exploitation of OBU and time relay. TDA improves the security of the network by improving the collision recognition rate and the broadcast rate. CSRP relies on the CS of the neighbor and the remaining energy of the OBU. When a node wants to broadcast a message, it initiates a CS request to its neighbors. These vehicles respond by either CS=0 (idle) or CS=1 (busy). Hence, the source node selects a set of all the vehicles with CS=0, computes both the distance d between it and the other one and the residual energy (RE) of its neighbors based on the initial and the consumption energy of the OBU. Then, the CSR Factor (CSRF) is computed so as to identify the optimal neighbor using the minimal residual energy and the least distance. Hence, a vehicle with the maximum CSRF is selected as the next optimal vehicle for transmission. The CSRF is updated through a series of observations. Therefore, the vehicle reaches the sin node in either one hop or in multiple hops.

3.3. HYBRID PROTOCOLS

3.3.1. SPBR

Secure Position-Based Routing (SPBR) for VANETs was presented in [34] where the authors incorporate mechanisms to assure the process of PBR and its operation, based on both cryptographic primitives and plausibility checks, with a view to reaching the stated security goals. These mechanisms use asymmetric cryptography and digital signatures for all messages. They adopt a public key infrastructure with a certification authority that issues both public and private key pairs, and certificates to vehicles. A certificate includes the node's public key, the attribute list, the CA identifier, the certificate lifetime and the CA signature. The list is used in order to differentiate between RSUs, public emergency vehicles and ordinary vehicles. Every received packet must have succumbed to a series of plausibility checks based on its timestamp and

location fields. The timestamp is used to guess the packet's availability. More checks are achieved by considering a maximum value of the transmission range, along with the node velocity. The maximal velocity is expected and the position of a vehicle is calculated with its speed and its previous location. If at least one check flunks, the packet is abandoned; else the packet is substantiated cryptographically. In the beginning, the certificate validity must be proved in case it was not already checked and hidden. In one hop communication, the source signature is the one requested. While in multi-hop communication, the packet is protected by two signatures. The first one is the source signature measured by the source close to the immutable fields. The second one is the sender signature produced by each node close to the mutable fields. After that, the signatures are authenticated. Contrarily to what was mentioned above, the packet is discarded if any of the signature authentications fail and the packet is subsequently processed. The authors suggest rate-limiting mechanisms in terms of the qualities of the sender node. A lower rate and a smaller transmission area are furnished for private vehicles compared to RSUs and to emergency vehicles. If the rate of such traffic originating from a node exceeds a protocol-specific threshold, its packets are not forwarded any further.

3.3.2. S-AMCQ

S-AMCQ designed by Eiza and al. is a Secure Ant-based Multi-Constrained QoS routing algorithm and was presented in [20]. S-AMCQ utilizes the Ant Colony Optimization (ACO) technique to calculate appropriate routes in VANETs depending on multiple QoS constraints dictated by the type of networking data transported by the network. In this proposal, every vehicle is recognized by its identity and receives a number of pseudonymous certificates from the CA and from the RSUs using the Pseudonymous Authentication Scheme (PAS) [35]. The Cryptographic information is saved in the TPD of each vehicle which must periodically diffuse a routine traffic message termed a Basic Safety Message (BSM) incorporating a vehicle's recent status. Thus, each vehicle can form an E-VoEG model of the vehicular network status and keep it up-to-date [34]. The E-VoEG model shows the local vehicular network topology that encircles each vehicle. The vehicle designates a foreseen lifetime and a pheromone value for each link in the model depending on the QoS requisites. In this the technique, several artificial ants construct solutions to an optimization problem that remind of the use of the real ones. The routing control ants decide which link is more reliable according to its pheromone and lifetime. At the beginning of the routing process, the source joins its signature to the Routing Request Ant (RQANT) message before broadcasting it. Then, the certificate is diffused and validated by the neighbors. If the RQANT does not meet all the plausibility checks, the message is rejected. Otherwise, a Routing Reply Ant (RPANT) is forwarded on the basis of the quality of the links that the RQANT has crossed. When a link breaks, a Routing Error Ant (REANT) is generated which encloses the ID of the immutable ant and the list of the nodes that have become unreachable in order to allow the source to initiate a new route discovery process. These plausibility checks are dedicated to defending the route discovery process against internal adversaries. For the external attackers, a digital signature mechanism is used to protect the routing control ants and to provide their integrity and authenticity.

4. COMPARISON OF THE VANET SECURE ROUTING PROPOSALS

4.1. CATEGORIZATION

The main objective of the above-presented approaches is to secure vehicular ad hoc routing. Those protocols could be categorized in chronological order into secure mechanisms based on cryptography, or on trust, or on both.

Table 1. Usage of security mechanisms by the proposals.

Solutions	Proposals	Secure Mechanism
Cryptography-based solutions	SEPPBR [23]	DS
	EMAP [24]	SC
	AMLA [25]	DS CS
	S-BRAVE [26]	CS
Trust-based solutions	MHLVP [28]	PC
	DAATM [29]	RS
	TM-AODV [30]	PC
	VSRP [31]	RS PC
	DRS [22]	RS PC
	EDTCP [32]	RS
	CSRP-TDA [33]	RS PC
Hybrid solutions	SPBR [34]	DS PC
	S-AMCQ [20]	CS PC

As precise in table 1, some protocols utilize more than one mechanism in order to reach various secure objectives. Table .2 gives the explicit name of each security mechanism.

Table 2. Notations.

Notation	Description
DS	Digital Signature
SC	Symmetric Cryptography
CS	Certificate Server
PC	Plausibility Checks
RS	Reputation System
PDR	Packet Delivery Ratio

4.2. COMPARISON OF THE DIFFERENT PROPOSALS

The main characteristics of the studied approaches and the performance aspects are summarized in Table 3. Characteristics comprise the security issues that have been addressed and the source of the approach which extends either from an existing routing protocol or from a brand-new one.

Table 3. Qualitative comparison of the surveyed protocols.

Proposal	Addressed security issues	Background	Network Throughput	PDR	Overhead	Scalability	Processing time
Cryptography-based solutions							
[23]	Authentication Data integrity Non repudiation	PBR	Good	Good	High	-	High
[24]	Authentication	New proposal	-	Good	High	Very high	Average
[25]	Authentication Non repudiation Integrity Anonymity	New proposal	-	Average	Low	Average	High
[26]	Authentication Integrity	BRAVE	-	Good	High	Average	Average
Trust-based solutions							
[28]	Integrity Reliability Availability Authentication Anonymity Confidentiality	New proposal	-	High	-	High	High
[29]	Data trust	New proposal	-	High	-	Average	-
[30]	Availability	AODV	Good	High	Average	-	-
[31]	Authentication Data trust	New proposal	-	Average	Low	High	-
[22]	Data trust	New proposal	-	High	-	High	-
[32]	Authentication	New proposal	-	High	-	High	Low
[33]		New proposal	High	Good	-	Average	Low
Hybrid solutions							
[34]	Authentication, Integrity Non repudiation	PBR	-	-	Low	Good	-
[20]	Authentication Integrity Non repudiation	New proposal	-	High	Low	Average	-

Performance aspects are based on network throughput, PDR, packet overhead, scalability and the level of CPU processing. The protocols are classified according to their apparition order for each security mechanism. It is clear that the performance evaluation differs from one proposal to another; it depends on the author's choices and on the security concerns treated. None of the above-mentioned proposals gave a complete performance evaluation of the approach since it is hard to deal with many VANETs requirements.

5. CHALLENGES AND OPPORTUNITIES

We are discussing whether the approaches that have been studied meet VANETs requirements and aim to answer the following questions:

1. Do the purposes of considered approaches conform to security objectives?
2. What are the challenges not addressed by each of the approaches?

The principal security objectives for routing are equivalent except privacy and anonymity. To achieve the same security objectives, the surveyed protocols apply different security mechanisms and different assumptions.

Most of the routing protocols experience operating problems with scalability when the number of nodes increases, when the high mobility and when the frequent topology changes [36-37]. The rise in the node number causes an enormous volume of information exchange to be generated on the network. Besides, each node that needs to maintain connection with others or to signal a packet is concerned with the frequent mobility changes. The use of symmetric cryptography is suitable for scalability because both communicating nodes share only one key [24]. Since VANETs have high application data requirements, the identification of malicious nodes is a great problem when using a shared key. To avoid this problem, VANETs have to furnish non-repudiation of the messages, using asymmetric cryptography based on two keys [23-25-38]. As known, VANETs access infrastructure via RSUs or Hot Spots, and the vehicles are registered with CA, which is suitable for asymmetric cryptography [39]. The CA guarantees the non-repudiation of messages because it manages the identities and credentials of all nodes registered with it. The critical disadvantage of asymmetric cryptography is the high level of processing which can cram the most important communication medium and yield DoS attacks [23-25]. With asymmetric cryptography, each packet is signed and this signature is verified by the CA. Each OBU requires saving a great number of anonymous public/private keys to sign traffic messages. If OBU's anonymous keys are revoked, it may take a long time to update the CRL which increments the time processing and produces network latency. To decline time delay, the nodes must be equipped with powerful hardware. Also the non-availability of the CA produces a break in the whole network connectivity.

Privacy and anonymity could be guaranteed with the usage of hashing functions [40-41]. Hash chains are employed to preserve mutable information such as hop-count. The signature can be created without connecting with the expected receiver. However, immutable information is guarded by digital signatures.

Secure routing does not need confidentiality because all information is visible by the intermediate nodes. Thus, any node can obtain the positions of the other nodes from the received packets. Confidentiality is mandatory when private information is swapped.

In the case of high mobility and in the absence of infrastructure, cryptography solutions cannot perform as well as expected. Indeed, classical cryptography solutions are overtaken by an authorized and authenticated user which becomes malicious. Hence, to fill the gap of cryptography against inside attackers, trust management is usually adopted [15]. Trust-based solutions use only vehicle-to-vehicle communication which cuts down the expense of road infrastructure. Trust management employs sensors in a reputation-based system or in plausibility checks using only vehicle-to-vehicle communication to address inside attackers [22-28-29-30-31].

In the reputation system mechanism, each vehicle is assigned a reputation score based on its behavior and feedback from other nodes. They are used to struggle against nodes agreed on, not

only against opponent nodes. But they are not adapted to scalability [29]. They have to follow the reputation of all nodes which need enormous tables of information that are hard to administrate and to keep up abreast.

Another possibility of defending against compromised nodes comes from plausibility. Plausibility checks mechanism aims to build a model for the current network at each node then checks the consistency of the received message contents against the network model. This check can be performed by comparing the data obtained from all the neighbors with the state of the surrounding environment obtained by sensors, or by pre-defined rules [1]. Plausibility verifies that a mechanism can be well dedicated to VANETs without degradation abatement of performance. To guarantee these checks, a prior model of the VANET must be proposed and embodied in each node.

The cryptographic schemes avoid attacks from compromised nodes. But the use of reputation systems with cryptography accomplishes better security against malicious nodes [20-34]. Also, the mechanisms that perform plausibility checks over the received data avoid compromised nodes, which enhances scalability and reduces mobility problems existing in reputation systems. Reputation systems generate extra communication overhead and introduce longer delays into the routing process. Hence, applying plausibility checks is preferable for VANETs.

Because of this, providing a secure routing protocol for VANETs must be guardedly examined while suitable countermeasures are taken.

6. CONCLUSIONS

In this paper, we performed a survey of several secure routing protocols by describing and comparing the studied approaches together. Post comparison of the existing approaches and analysis of the VANET needs leads us to conclude that a security mechanism depends not only on the level of efficiency but also on the network constraints.

VANETs environments are based on strong assumptions which facilitate the design of a secure routing protocol. These assumptions allow choosing an approach which combines cryptography and trust-based solutions as the most appropriate scheme for VANETs. Asymmetric cryptography provides the non-repudiation of messages. Symmetric cryptography based on hash functions enhances privacy and anonymity. The plausibility check technique protects against compromised and sinkhole nodes besides not affecting the performance of VANETs while correcting the inappropriate detected information.

Although research on VANETs bears great importance worldwide, there are still many issues that have courteous attention. The most important one is location privacy because of the direct relationship between driver and vehicle. The attacker can act on a driver's privacy. We can cite as an example of the tracking of its location. Also, GPS spoofing needs to be addressed to prevent an attacker from bringing false readings in GPS devices. As a result, more research must be carried out to find more suitable secure routing protocols for VANETs. Finally, since defining an efficient routing protocol for all VANETs applications is very difficult, it is beneficial to apply several security schemes when designing a secure routing protocol to adapt to the various requirements of applications.

In the light of the synthesis we performed across this survey, the various challenging issues revealed regarding VANET secure routing can be addressed within a deeper work whose target will be to design a coherent and sufficient secured VANET routing proposal.

REFERENCES

[1] Emanuel Fonseca and Andreas Festag, "A Survey of existing approaches for secure Ad Hoc routing and their applicability to VANETS", NEC Technical Report NLE-PR-2006-19, NEC Network Laboratories, March 2006.

[2] Ankit Kumar and Madhavi Sinha, "Overview on vehicular ad hoc network and its security issues", International Conference on Computing for Sustainable Global Development (INDIACom), March 2014.

[3] A.P. Jadhao and D. N. Chaudhari, "Security Aware Routing Scheme In Vehicular Adhoc Network", 2nd International Conference on Inventive Systems and Control (ICISC), January 2018.

[4] Wenjia Li and Houbing Song, "ART: An Attack-Resistant Trust Management Scheme for Securing Vehicular Ad Hoc Networks", IEEE Transactions on Intelligent Transportation Systems , vol. 17, issue 4, April 2016.

[5] Nirav J. Patel and Rutviji H. Jhaveri, "Trust based approaches for secure routing in VANET: A Survey", International Conference in Advanced Computing Technologies and Applications (ICACTA-2015), March 2015.

[6] Ram Shringar Raw, Manish Kumar and Nanhay Singh, "Security Challenges, Issues and Their Solutions for VANET", International Journal of Network Security & Its Applications (IJNSA), vol. 5, no. 5, September 2013.

[7] Sofiene Djahel, Ronan Doolan, Gabriel-Miro Muntean and John Murphy, "A Communications-Oriented Perspective on Traffic Management Systems for Smart Cities: Challenges and Innovative Approaches", IEEE Communications Surveys & Tutorials, vol. 17, issue 1, July 2014.

[8] Rashmi Mishra, Akhilesh Singh and Rakesh Kumar, "VANET Security: Issues, challenges and solutions", International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), March 2016.

[9] Mr.Nikhil, D.Karande, Ms.Kushal and K.Kulkarni, "Efficient routing protocols for vehicular adhoc network", International Journal of Engineering Research & Technology (IJERT), vol. 2, issue 1, January 2013.

[10] Sridevi Hosmani and Basavaraj Mthpati, "Survey on Cluster Based Routing Protocol in VANET", International Conference on Electrical, Electronics, Communication, Computer, and Optimization Techniques (ICEECCOT), December 2017.

[11] Sachin Godse and Parikshit Mahalle, "Secure & Efficient Routing Mechanisms in VANET Using CBDS", International Conference on Computing, Communication, Control and Automation (ICCUBEA), August 2017.

[12] Anup Dhamgaye and Nekita Chavhan, "Survey on security challenges in VANET", International Journal of Computer Science and Network (IJCSN), vol. 2, issue 1, January 2013.

[13] Chun-I Fan, Wei-Zhe Sun, Shih-Wei Huang, Wen Shenq Juang and Jheng-Jia Huang, "Strongly Privacy-Preserving Communication Protocol for VANETs", 9Th Asia Joint Conference on Information Security (asia jcis)", September 2014.

[14] Danda B. Rawatz, Bhed B. Bistax, Gongjun Yan and Michele C. Weigley, "Securing Vehicular ad-hoc networks against malicious drivers: a probabilistic approach", International conference on Complex Intelligent and Software Intensive Systems (CISIS), July 2011.

[15] Chaker Abdelaziz Kerrache, Carlos T. Calafate, Juan-Carlos Cano, Nasreddine Lagraa and Pietro Manzoni, "Trust management for Vehicular Networks: An Adversary-Oriented Overview", IEEE Access, vol. 4, issue 2, December 2016.

[16] Sumegha C. Sakhreliya and Neha H. Pandya, "PKI-SC: Public key infrastructure using symmetric key cryptography for authentication in VANETs", IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), December 2014.

[17] Mohamed Nidhal Mejri, Jalel Ben-Othman and Mohamed Hamdi, "Survey on VANET security challenges and possible cryptographic solutions", Vehicular Communications, vol. 1, issue 2, April 2014.

[18] M. Alimohammadi and A. A. Pouyan, "Performance Analysis of Cryptography Methods for Secure Message Exchanging in VANET", International Journal of Scientific & Engineering Research, vol. 5, issue 2, February 2014.

[19] Raghu Sunnadkal, Ben Soh and Hien Phan, "A four-stage design approach towards securing a vehicular ad hoc networks architecture", 5th IEEE International Symposium on Electronic Design, Test and Application (DELTA), January 2010.

[20] Mahmoud Hashem Eiza, Thomas Owens and Qiang Ni, "Secure and Robust Multi-Constrained QoS Aware Routing Algorithm for VANETS", IEEE Transactions on Dependable and Secure Computing, vol. 13, issue 1, February 2016.

[21] Martin Ring and Reiner Kriesten, "Plausibility Checks in Automotive Electronic Control Units to Enhance Safety and Security", The Fifth International Conference on Advances in Vehicular Systems, Technologies and Applications, November 2016.

[22] Jared Oluoch, "A Distributed Reputation Scheme for Situation Awareness in Vehicular Ad Hoc Networks (VANETs)", IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support (CogSIMA), March 2016.

[23] Jie Hou, Lei Han, Jiqiang Liu and Jia Zhao, "Secure and efficient protocol for position-based Routing in VANETs", IEEE International conference on Intelligent Control Automatic Detection and High-End Equipment (ICADE), July 2012.

[24] Wasef, A. and Xuemin Shen, "EMAP: Expedite Message Authentication Protocol for vehicular ad Hoc networks", IEEE Transactions on Mobile Computing, vol.12, issue 1, January 2013.

[25] Bhavesh N.Bharadiya, Maity Soumyadev and Hansdah R.C., "A protocol for authentication with multiple levels of anonymity (AMLA) in VANETs", 27th International conference on Advanced Information Networking and Applications Workshops (WAINA), March 2013.

[26] Juan A. Martinez, Daniel Vigueras, Francisco J. Ros and Pedro M. Ruiz, "Evaluation of the use of guard nodes for securing the routing in VANETs", Journal of Communications and Networks (JCN), vol. 15, issue 2, April 2013.

[27] Pedro M. Ruiz, Victor Cabrera, Juan A. Martinez and Francisco J. Ros, "BRAVE: Beacon-less Routing Algorithm for Vehicular Environments", the 7th IEEE International Conference on Mobile Adhoc and Sensor Systems (MASS), November 2010.

[28] Osama Abumansoor and Azzedine Boukerche, "A secure cooperative approach for nonline-of-sight location verification in VANET", IEEE Transactions on Vehicular Technology, vol. 61, issue: 1, January 2012.

[29] Tahani Gazdar, Abderrezak Rachedi, Abderrahim Benslimane, and Abdelfettah Belghith, "A distributed advanced analytical trust model for vanets", 2012 IEEE Global Communications Conference (GLOBECOM), December 2012.

[30] A.Chinnasamy , S.Prakash and P.Selvakumari, "Enhance trust based routing techniques against sinkhole attack in AODV based VANET", International Journal of Computer Applications, vol. 65, issue 15, March 2013.

[31] Sanjay K. Dhurandher, Mohamed S. Obaidat, Amrit Jaiswal, Akanksha iwari and Ankur Tyagi, "Vehicular Security Through Reputation and Plausibility Checks", IEEE Systems Journal, vol. 8, issue 2, June 2014.

[32] Tahani Gazdar, Abdelfettah Belghith, and Hassan Abutar, "An Enhanced and Distributed Trust Computing Protocol for VANETs", IEEE Access, vol. 6, pp. 380-392, October 2017.

[33] Amr Tolba, "Trust-Based Distributed Authentication Method for collision Attack Avoidance in VANETs", IEEE Access, vol. 6, pp. 62747-3536, October 2018.

[34] Charles Harsch, Andreas Festag and Panos Papadimitratos, "Secure position-based routing for VANETs", 66th IEEE Vehicular Technology Conference (VTC), October 2007

[35] Yipin Sun, Rongxing Lu, Xiaodong Lin, Xuemin Shen and Jinshu Su, "An Efficient Pseudonymous Authentication Scheme With Strong Privacy Preservation for Vehicular Communications", IEEE Transactions on Vehicular Technology, vol. 59, issue 7, September 2010.

[36] Belal Amro, "Protecting Privacy in VANETs Using Mix Zones with Virtual Pseudonym Change", International Journal of Network Security & Its Applications (IJNSA), vol. 10, no. 1, January 2018.

[37] Marvy B. Mansour, Cherif Salama, Hoda K. Mohamed and Sherif A. Hammad, "VANET Security and Privacy - An Overview", International Journal of Network Security & Its Applications (IJNSA), vol. 10, no. 2, March 2018.

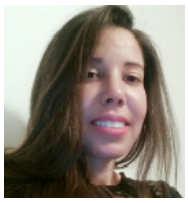
[38] Mahmoud Hashem Eiza, and Qiang Ni, "An Evolving Graph-Based Reliable Routing Scheme for VANETs", IEEE Transactions on Vehicular Technology, vol. 62, issue 4, May 2013.

[39] Tahani Gazdar, Abderrahim Benslimane, and Abdelfettah Belghith, "Secure Clustering Scheme Based Keys Management in VANETs", 2011 IEEE 73rd Vehicular Technology Conference (VTC Spring), May 2011.

[40] An-Ni Shen , Song Guo, Deze Zeng and Guizani M. "A lightweight privacy-preserving protocol using chameleon hashing for secure vehicular communications", IEEE Wireless Communications and Networking Conference (WCNC), April 2012.

[41] Biswas S. and Misic, J., "A cross-layer approach to privacy-preserving authentication in WAVE-enabled VANETs", IEEE Transactions on Vehicular Technology, vol. 62, issue 5, June 2013.

AUTHORS



Afef Slama is an Assistant at the Higher School of Economic and Commercial Sciences of Tunis since 2016. She received her Master Degree in Computer Science from the Tunisia Polytechnic School in 2012. She is currently working toward the Ph.D. degree with the University of Manouba. Her research interests include performance evaluation and simulation of network protocols in VANETs. She is currently a research member in HANA research group.

Ilhem Lengliz is an Assistant Professor at the Military Academy since 2008. She received her Engineer Degree and PhD in Computer Science from the University of Manouba respectively in 1991 and 2001.Her research interests are in congestion control, performance evaluation and simulation of network protocols (transport and routing), mainly in mobile ad hoc environments (MANETs, VANETs and WSNs). She is also interested in security aspects related to the deployment of such protocols. She is currently a senior research member in HANA research group where she supervises master and PhD students.