SECURITY FRAMEWORK FOR VANET: SURVEY AND EVALUATION

Emad Felemban[1†], Salem M. Albogamind[2], Atif Naseer[3] and Hassan H. Sinky[4††],
eafelemban@uqu.edu.sa S43580002@st.uqu.edu.sa anahmed@uqu.edu.sa hhsinky@uqu.edu.sa
Umm Al-Qura University, Makkah, Saudi Arabia

Summary
In the last few years, the massive development in wireless networks, high internet speeds and improvement in car manufacturing has shifted research focus to Vehicular Ad-HOC Networks (VANETs). Consequently, many related frameworks are explored, and it is found that security is the primary issue for VANETs. Despite that, a small number of research studies have taken into consideration the identification of performance standards and parameters. In this paper, VANET security frameworks are explored, studied and analysed which resulted in the identification of a list of performance evaluation parameters. These parameters are defined and categorized based on the nature of parameter (security or general context). These parameters are identified to be used by future researchers to evaluate their proposed VANET security frameworks. The implementation paradigms of security frameworks are also identified, which revealed that almost all research studies used simulation for implementation and testing. The simulators used in the simulation processes are also analysed. The results of this study showed that most of the surveyed studies used NS-2 simulator with a percentage of 54.4%. The type of scenario (urban, highway, rural) is also evaluated and it is found that 50% studies used highway urban scenario in simulation.

Key words:
Vehicular Ad-HOC Networks (VANETs), Security Framework, urban scenario.

1. Vehicular Ad-hoc Networks

One of the important domains in the computer and network science is communication between vehicles. This communication could be achieved with the use of Vehicular Ad-Hoc Networks (VANETs), which is similar to Mobile Ad-Hoc Networks (MANETs) used for transferring information between vehicles (Vehicle-to-Vehicle (V2V) communications) and Roadside Units (RSUs) referred as Vehicle-to-Infrastructure (V2I) communications [24], [25] (See Fig. 1). The main goal for VANETs is providing comfort and safety for passengers. To achieve this goal, electronic devices such as Wireless modem, Global Positioning System (GPS) and sensors should be placed inside vehicles to provide VANET communication.

Manuscript received August 5, 2021
Manuscript revised August 20, 2021
https://doi.org/10.22937/IJCSNS.2021.21.8.8

1.1 VANET Architecture

Generally, Wireless Access in Vehicular Environment (WAVE) is used for communication among vehicles and RSUs. It updates about traffic flow and vehicle information to ensure pedestrian and driver safety. It also improves performance of traffic management system. The VANET comprises of several units such as On-board unit (OBU), Roadside Unit (RSU) and Trust Authority (TA) [26].

1) Roadside Unit (RSU): It is a computing device mounted on roadside, road intersection, parking area or some specific location [27]. It uses IEEE 802.11p radio technology to provide dedicated short-range communication (DSRC) for network devices in it. RSU offers local connectivity to passing vehicles. It can also communicate with other network devices.

2) On-board unit (OBU): It is a tracking device to collect location, acceleration, and speed information in vehicle. It uses GPS and share vehicle information with RSUs through wireless link of IEEE 8022.11p. The main components of OBU include sensors, read/write memory, user interface and Resource Command Processor (RCP). This unit take power from vehicle battery. Fig. 2 shows its details.

Trust Authority (TA): TA is responsible for vehicle identification, secure authentication, and authorization

1.2 Communication Methods

VANET is a main application of Intelligent Transportation Systems (ITS). In ITS, vehicles can communicate with other vehicles and with other infrastructures. ITS is responsible to provide road safety, overcome traffic congestion and improve traffic flow by utilizing features of VANETs. Fig. 3 shows communication in VANETs.
Vehicle-to-everything (V2X) communications help to ensure traffic safety in ITS. It provides real time information about road congestion, emergency situations and collision warnings [28]. It can also exchange information among vehicles and vehicle to pedestrians

(V2P) infrastructures. In V2V communication, vehicles can broadcast useful event information among each other. The transmission medium has low latency and high transmission rate.

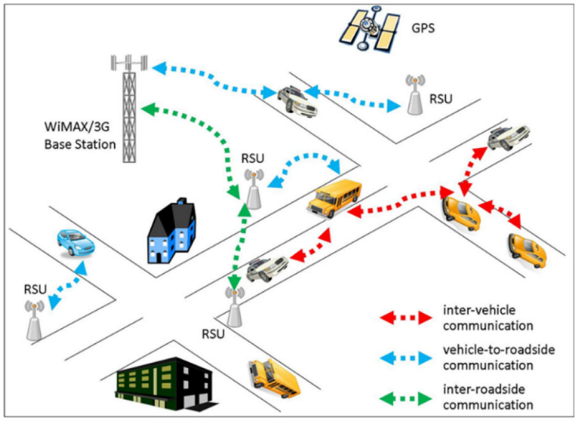

Fig 1. Vehicular Ad-Hoc Network

Vehicle-to-Infrastructure (V2I) communication can exchange information between vehicles and other networks. It requires high bandwidth than V2V to establish connection with RSUs and infrastructures [30].

The communication in VANET can be classified into four categories namely warning message propagation, V2V group communication, vehicle beaconing and infrastructure to vehicle warning [34]. Warning messages are used to notify a vehicle or a group of vehicle about some critical event e.g accident, collision or congestion. This message should propagate on only those vehicles which are heading toward that location to avoid traffic jams. It requires a routing algorithm which first finds targeted vehicles and then send this warning message to them [34].

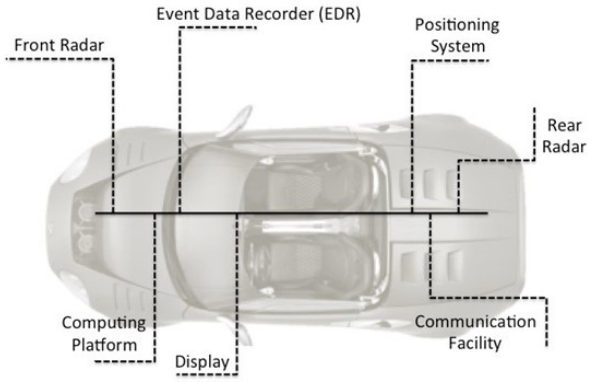

Fig 2. On-board Unit (OBU)

In V2V group communication, only vehicles from same brand and location can participate. Vehicles which have some identical features can also participate in V2V group communication. Vehicle beaconing is the beacon message sent to nearby vehicles to share acceleration, velocity and speed of source vehicle. Infrastructure to Vehicle warning messages is issued from RSUs to nearby vehicles when a critical event is detected e.g collision in a narrow or curved road.

Recently, Cellular vehicle-to-everything (C-V2X) is introduced which provides a connectivity platform to support V2X communications [31]. The C-V2X technology [32] was developed in third-generation partnership project (3GPP) [48]. It connects vehicles to cooperative intelligent transport systems (C-ITS) that reduces traffic congestion.

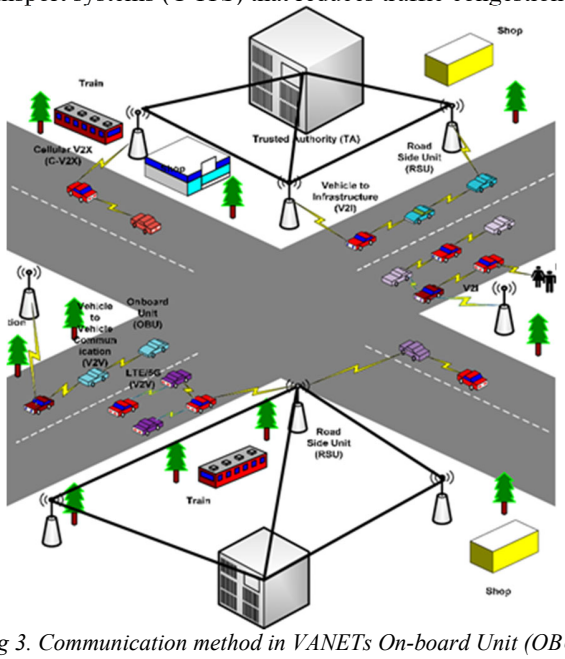

Fig 3. Communication method in VANETs On-board Unit (OBU)

1.3 VANET Characteristics

VANETs offer many reliable services with limited access to network infrastructure. The characteristics of VANETs are discussed below.

- High Mobility: It is the main feature of VANETs. In VANETs, vehicle follow road direction, which makes it different from other Adhoc networks where nodes can move freely in random direction. Many researchers explored this special feature [35]. The highly mobile nodes reduce communication time among vehicles because the get out of each other's communication range quickly [36].
- Dynamic Network Topology: The topology changes rapidly in network. It results in difficulty in recognizing a particular vehicle.
- Wireless Communication: It is responsible for secure communication during transmission through a wireless medium [29].

- Limitation of Transmission Power: VANETs use WAVE for transmission which has limited power. It ranges from 0 to 28.8 dBm in 1 Km [37].
- Driver Safety: VANETs allow applications which can communicate directly between vehicles and with RSUs. It improves traffic flow, passenger comfort and driver safety.
- Large Network: VANETs consists of a large network on highways and toll tax points [38].
- Network Strength: It depend on traffic flow. In case of traffic jam it is very high.
- Volatility: The connections in VANETs are volatile in nature. Due to high mobility, the connection among vehicles is lost quickly [39].

As any newly evolving networking system, VANET has its own challenges related to security. Traffic safety is a major objective of VANET. It should work on a complete secure echo system to avoid any vandalism, hijacking or denial of service attacks. There are many surveys available in literature which focused on the privacy schemes in VANETs.

1) Study and survey literature for security frameworks of VANETs.

2) Define a list of evaluation parameters that are used to evaluate these frameworks.

3) Categorize the resulting evaluation parameters based on context application.

4) Summarize the details of the frameworks from three perspectives including application type (simulation or real), used simulators and application scenario.

The remaining part of this paper is structured as follows: In Section 2, we discuss literature review. Section 3 describes re-search methodology. Section 4 presents result and discussions. Finally, we conclude the paper and provide future research directions in Section 5.

2. Literature Review

The related state-of-art research studies are analyzed and summarized in this section. The Survey in [42] comprehensively discusses architecture, security, challenges, and possible solutions for secure communication in existing methods for VANETs. It also includes authentication schemes, mobility, and other network simulators. A few safety applications of VANETs are also presented. The research [43] investigated the elements of VANETs and addressed challenges for reliable wireless communication. The taxonomy of routing protocols, strengths and limitations of these protocols are also discussed for VANETs. It also compared IEEE 802.11p and Long-Term Evolution (LTE) technologies for vehicle networking.

The authors in [51] reviewed routing protocols with emphasis on authentication and security mechanisms for secure VANET communication. In [55], the researcher described security components of the VANETs, analyzed latest research trends to deal with security vulnerabilities and proposes future research directions. The research study of [52] discussed

applications, security requirements, security and protection issues, validation schemes and challenges in VANETs. The author in [49] reviews existing efforts for attacks mechanisms, security requirements and challenges in VANETs.

The study in [50] described nature of attacks on security goals. It also classified them into different levels based on security goals. The study [41] presented characteristics of attacks and threats in VANETs. The location-based privacy schemes are presented along with trust management models. The evolution from the VANETs to VCC is covered and discussed the architecture, the security and privacy issues in VCC. The survey study [29] focus on security frameworks for VANETs. The first part presented overview of VANET, security characteristics, challenges and requirements. The second part focused on classification of different attacks and their related solutions. The third part is a comparison of these solutions in VANET. Study [53] discussed different approaches used to prevent collision in VANETs. [40] summarized recent developments to deal security attacks to ensure secure communication. The applications and authentication schemes are also introduced. In [44] the researchers went through VANETs' vulnerabilities and attacks. They surveyed and examined some recent security solutions along with their achievements and limitations.

The authors in [45] focused on the routing protocols and discussed latest advancements on VANETs routing. The researchers provide vulnerabilities and attacks which can affect the performance of VANETs. [46] reviewed some popular architectures of VANETs, WAVE by IEEE, C2C-Net by C2C consortium / GeoNet and CALIM by ISO. It also discussed safety related application protocols such as WSMP by WAVE and CALM FAST by ISO. [47] introduced broadcasting, different performance and QoS related issues in VANETs. It provided a comparative study of QoS-aware broadcasting protocols and their taxonomies. In [48], the researchers described various applications and authentication schemes used in the VANET. Security requirements of these schemes are listed and analyzed.

From the above listed state-of-the-art works, it is observed that most of the surveys didn't opt to cover whole security frameworks for VANETs, rather, they only covered fewer as-pects of VANET's security, which led in turn to

make the analysis related to these studies a bit directed and not holistic, hence the parameters mentioned in those studies can't be generalized to be a method for evaluation for newly developed security frameworks. Examples of such studies are the following: [40], [45], [46] and [47]. The way some studies tended to use in the evaluation of some security parameters is descriptive, which means the analysis followed in the measurement of these parameters is a qualitative one, not a quantitative one, and this leads to making the parameters not measurable if used in any future evaluation process. Examples of such studies are: [41], [44], [51], [22], [52], [53] and [54].

The research studies [42], [55] and [43], didn't specify the evaluation parameters clearly, they just provided general findings without going in details through the parameters that are being analyzed, which makes the evaluation process ambiguous and not obviously based on measurable parameters.

Having the above analysis of the literature review leads to a clear need to have a research that is fully dedicated for the purpose specifying clear parameters to evaluate future security frameworks of VANETs and the need for these parameters to be categorized in their application context in order to give researchers the opportunity to provide proofed judgments on future proposed security frameworks.

3. Research Methodology

This section discusses the methodology used to carry out this research. It includes surveying previous studies on VANET security frameworks, studying and analyzing these frameworks.

The main parameters are extracted which affect security process of those frameworks. Since these parameters are used to evaluate the frameworks from a processing perspective, they can also be used to evaluate other security frameworks. Hence, a list of the parameters is created that are present in these frameworks and categorized into groups relevant to their application context.

Our research started by surveying fifty-four previous re-searches that revealed full or partial security frameworks for VANETs. Twenty-three out of the fifty-four research studies included clearly stated parameters that showed to be effective in measuring the performance of those security frameworks. The research studies are surveyed in detail and all parameter used in measuring the performance of those frameworks are extracted and their final count reached ninety-one parameter. The list of parameters is provided in Table. 1.

The ninety-one parameters that were extracted from the VANET security-frameworks' studies were analyzed after-ward. During this analysis, some parameters were mentioned with different names in different studies although they have the same meaning. Hence, these identical-meaning parameters were grouped under one common name, and some the parameters were excluded due to being irrelevant to the study context. result was a list of forty parameters, which had different meaning and found relevant to research context. The resulting set of evaluation parameters are listed in section 4.

4. Result and Discussion

The results of this research study are presented which includes the main resulting set of extracted evaluation parameters. It also includes categorization of these parameters into more informative and handy categories. These parameters are defined to give clear idea about their relationship with security function. These definitions are either extracted from the respective research studies or defined using external references. The list of parameters definitions is provided below:

1) Processing delay: The time taken to process data packets during transmission in network [8,17] .
2) Tracking time of attackers: It is the time required identify attack and locate attacker which violate security of the network [1].
3) Network recovery time: The time taken by network to recover from attack [1].
4) Repairability time: It is a measure of time taken for attack identification and prevention in network [1].
5) False alarm detection rate: It shows the ratio of attacks identified by system to total number of attacks in network [1].
6) Spoofed packet detection: It measures spoofed identities detected as compared to their actual number introduced by attacker [1].
7) Packet loss rate: Packets of information be unsuccessful to achieve destination, particularly in circumstances of congestion [12,19].
8) Communication overhead: The overheads identified during attack detection and its prevention mechanisms [1,13].
9) Throughput: It is a measure of successful message delivered in a communication channel [15,16].
10) End to End delay: The time taken by a message to reach its destination [19,23].
11) Verification delay: Time overhead to perform the pro-cess of the aggregate signature verification [3,9].
12) Packet delivery rate: The number of data packets received by destination nodes divided by the number of data packets transmitted by source nodes [3,4,5,19].

Table 1. LIST OF PRIMARY PARAMETERS

No	Parameters	No	Parameters	No	Parameters	No	Parameters	No	Parameters
1	Processing Delay	19	Packet Loss Rate	37	Computation Time	55	Average End-To-End Delay	73	Channel Busy Time
2	Network Recovery Time	20	Performance	38	Message Delivery Rate	56	Dissemination Efficiency	74	Overall Packet Delivery Ratio
3	Tracking Time of Attackers	21	Security Level	39	Message Overhead Analysis	57	Number of Collision	75	Average Per Vehicle Throughput
4	Reparability Time	22	Route Discovery	40	Verification Delay Analysis	58	Average Speed	76	Routing Efficiency
5	Spoofed Packet Detection	23	QoS Routing	41	Packet Delivery Ratio	59	Travelling Time	77	Authentication Delay
6	False Alarm Detection Rate	24	Mean Opinion Score (Mos)	42	Average Number of Clusters	60	Average Distance	78	Keying Overhead
7	Drop Percentage	25	Overall Percentage Detected Trusted	43	Jitter	61	Number of Packets	79	Detection Accuracy
8	RSU Genetic Value	26	Overall Percentage Detected Malicious	44	Packet Dropped Ratio	62	Goodput	80	Throughput of Drop Pkt
9	Communication Overheads	27	Percentage of Detected Vehicles Per Layer	45	Message Signing Cost	63	Ratio of Packet Loss	81	Throughput of Sending Bits
10	Throughput	28	Overall Delay to Detect A Trusted Vehicle	46	Message Verification Cost	64	Average Delay	82	Throughput of Forwarding Packet
11	Error Rate	29	Overall Delay to Detect A Malicious Vehicle	47	The Average Message Delay	65	Network Lifetime (Nlt)	83	Vehicle Density
12	Processing Time	30	Average Delay of Detection Per Layer	48	Average Message Loss Ratio	66	Energy Consumption (Ec)	84	Average Speed of The Ambulance
13	End to End Delay	31	Consistency of Computed	49	Packet Drop	67	Security Analysis	85	Average Cumulative Jitter
14	Verification Delay	32	Average Trust Metric of a Malicious Vehicle	50	Overhead	68	Delivery Probability	86	Average PSNR
15	Packet Delivery Rate	33	Vehicle Density	51	Redundancy Rate	69	Overhead Ratio	87	Handoffs Frequency
16	Network Latency	34	Computational Delay Of RSU	52	Total Number of Beacons	70	Latency	88	Monetary Cost
17	Computational Delay	35	Centrality Measures	53	Packet Loss Ratio	71	Transmit Power	89	Detection Ratio
18	Failure Rate	36	Data Traffic	54	Propagation Distance	72	Average Channel Access Time	90	Relay Ratio
								91	Delay

13) Network latency: The latency is the measure of the average delay in the network from when a message is created to when it is finally received at its destination [3].

14) Failure rate: Rate of failed verification's using the aggregate signature verification to the total verification's [3].

15) Route discovery: The average time for processing a request to find the best available route from the source to the destination, when sending a message [5,19].

16) QoS Routing: It is a routing mechanism to ensure required QoS level within network. It finds and selects the optimum path during traffic flow [5].

17) Mean Opinion Score (MOS) : A measure representing overall quality of QoS Routing from source to destination [5].

18) Overall percentage of detected trusted vehicles: Ratio of detected trusted vehicles to actual trusted vehicles [6].

19) Overall percentage of detected malicious vehicles: Ratio of detected malicious vehicles to actual malicious vehicles [6].

20) Overall delay to detect a trusted vehicle: Average duration to detect a trusted vehicle vs. number of hops [6].

21) Overall delay to detect a malicious vehicle: Average time to detect a malicious vehicle vs.

number of hops [6]. Vehicle Density: It is the number of vehicles per unit area of road [7].

22) Computational delay of RSU: Computation overhead of roadside Infrastructure [3].
23) Centrality measures: This value shows the role of node within network. It is highest for central node [7].
24) Data Traffic: Data traffic denotes the data transmitted between the vehicles (measured in kbps) [7].
25) Message Overhead: It is part of the message that is not useful in the communication [9].
26) Jitter: It is the measure of variation time in packet arrival [12,19].
27) Authentication Delay: Time overhead to perform the authentication process [21].
28) Redundancy rate: It is the ratio of replicated messages to all the messages in network [14].
29) Total number of beacons: It refers to total beacons generated during transmission [14].
30) Packet loss ratio: It is the proportion of collisions during transmission [14].
31) Average Speed: It is the average speed of the vehicle during travelling [7].
32) broadcasts/unit time. It increases if the message is distributed farther [14].
33) Network Life Time (NLT): The failure time of the first sensor node [18].
34) Energy Consumption (EC): Amount of energy consumed during the cryptography process [18].
35) Keying Overhead: It is the time overhead to generate the keys [21].
36) Detection Ratio: The ratio of detection of grey vehicles to the total vehicles [21,23].
37) Throughput of Drop Packet: Number of packets dropped in [22].
38) Throughput of Sending Bits: Amount of sent bits [22].
39) Throughput of Forwarding Packet: Number of forwarding packets in presence of malicious nodes [22].

The context where each of the resulting parameters are mentioned determines the best way to apply measurement on this parameter. The evaluation of proposed framework has significant importance. The list of surveyed research studies and their respective parameters are included in Table. II. The resulting set of parameters is categorized into three main categories i.e General, Network and Security. This categorization process is needed to provide related parameter list based on orientation of frameworks. Table. III lists the parameters and their respective categories. It is very important to specify a suitable testing environment while testing the applicability and effectiveness of security frameworks. An application environment can either be practical, real or simulation based. Table. IV provides listing of application environments used through the surveyed studies.

Table 2. LIST OF RESEACH ARTICLES AND THEIR EVALUATIONPARAMTERS

S. No	Paper Title	Parameters Evaluated
1	Genetic-based framework for prevention of masquerade and DdoS attacks in vehicular ad-hoc networks [1]	Processing delay, Network recovery time, Tracking time of attackers, Reparability time, Spoofed packet detection, False alarm detection rate, Drop percentage, Communication overheads
2	Design and development of Secured Framework for Efficient Routing in Vehicular Ad-Hoc Network [2]	Throughput , Processing Time, End to End delay
3	Privacy-Preserving authentication framework using bloom filter for secure vehicular communications [3]	Verification delay , Packet delivery rate, Network latency, Throughput, Failure rate, Packet loss rate, Computational delay of RSU
4	A privacy-preserving distance-based incentive scheme in opportunistic VANETs [4]	Packet delivery Rate , End-to-end delay
5	A multi constrained QOS routing algorithm for vehicular ADHOC network [5]	Packet delivery rate, route discovery , QoS Routing, Mean Opinion Score (MOS)
6	DTCF: A distributed Trust Computing Framework for Vehicular Ad hoc Network [6]	Percentage detected trusted/malicious ,Overall delay to detect a trusted/malicious vehicle
7	Reinforcing VANET Security using Ant Colony Optimization through Heuristic Approach [7]	Vehicle, Average Speed, Centrality measures, Data Traffic
8	Secure Vehicle Communication Using ID Based Signature Scheme [8]	Packet Delivery Ratio, Delay, Computation Time
9	A Novel RSU-Aided Hybrid Architecture for Anonymous Authentication (RAHAA) in VANET [9]	Message Overhead, Verification Delay
10	An Efficient and Secured Routing Protocol for VANET [10]	Packet Delivery Ratio, Normalized Routing Load
11	An Efficient Mutual Authentication Framework with Conditional Privacy Protection in VANET [11]	Computation Overhead, Communication costs
12	D&PMV: New Approach for Detection and Prevention of Misbehave/Malicious Vehicles from VANET [12]	Throughput, Delay, Jitter, Packet Dropped Ratio
13	Group Key Authentication scheme for VANET Intrusion detection (GKAVIN) [13]	Delay, Delivery Ratio, Packet Drop, Overhead
14	Lion optimization algorithm (LOA)-based reliable emergency message broadcasting system in VANET [14]	Redundancy rate, Total number of beacons, packet loss ratio, Propagation distance, average end-to-end delay, Dissemination efficiency, delivery ratio
15	Performance Evaluation of V2Vcommunication by Implementing Security Algorithm in VANET [15]	Throughput, Delay
16	Reliability refinement in VANET with hybrid jamm18ing attacks using novel index-based voting algorithm [16]	Throughput, end to end Delay, Packet Delivery Ratio
17	SCICS: A Soft Computing Based Intelligent Communication System in VANET [17]	Average Delay, Processing time
18	Secure Data Transmission Through Reliable Vehicles in VANET Using Optimal Lightweight Cryptography[18]	Network Life Time, Packet Delivery Ratio, Energy Consumption
19	Towards a Trusted Vehicular Routing in VANET [19]	Throughput, Packet loss rate, Packet delivery rate, Jitter, Delay, Routing efficiency
20	Traffic Information Dissemination System: Extending Cooperative Awareness Among Smart Vehicles with only Single-Hop Beacons in VANET [20]	Packet delivery ratio, End-to-end delay , Packet loss
21	Trust based authentication technique for cluster based vehicular ad hoc networks (VANET) [21]	Packet Delivery Ratio, Authentication Delay, Keying Overhead, Detection Accuracy, Delivery Ratio
22	TruVAL: Trusted Vehicle Authentication Logic for VANET [22]	Throughput of Drop Packet, Sending Bits and Forwarding Packet
23	Vtrust: A Robust Trust Framework for Relay Selection in Hybrid Vehicular Communications [23]	Detection Ratio, Relay Ratio

All surveyed studies used simulation-based environments for the application of VANET security frameworks. The main reason behind this is the difficulty in implementation of a real application scenario for security/technical reasons when VANETs are under development and testing. Many simulators can be used when it comes to implementation of VANET, however, it can be tricky to choose a good simulator to use. There are many simulators that have been used in the implementation of VANET security frameworks. Table. IV gives insight to these simulators. In the surveyed studies, 54.5% studies used NS-2 as their simulator of choice, which indicates that this open-source simulator is probably the most suitable for the implementation of VANET frameworks.

No.	Parameter	Kind of Parameters			No.	Parameter	Kind of Parameters		
		General	Network	Security			General	Network	Security
1	Processing delay		1		21	Delay to detect a malicious vehicle			1
2	Network recovery time			1	22	Vehicle Density	1		
3	Tracking time of attackers			1	23	Computational delay of RSU		1	
4	Reparability time			1	24	Centrality measures		1	
5	Spoofed packet detection			1	25	Data Traffic		1	
6	False alarm detection rate			1	26	Message Overhead		1	
7	Packet loss rate		1		27	Jitter		1	
8	Communication overheads			1	28	Authentication Delay			1
9	Throughput		1		29	Redundancy rate		1	
10	End to End delay		1		30	Total number of beacons		1	
11	Verification delay			1	31	Packet loss ratio		1	
12	Packet delivery rate		1		32	Dissemination efficiency		1	
13	Network latency		1		33	Average Speed Vehicle	1		
14	Failure rate			1	34	Network Life Time (NLT)		1	
15	Route discovery		1		35	Energy Consumption (EC)			1
16	QoS Routing		1		36	Keying Overhead			1
17	Mean Opinion Score (MOS)		1		37	Detection Ratio			1
18	Overall percentage detected trusted			1	38	Throughput of Drop Pkt			1
19	Overall percentage of detected malicious vehicles			1	39	Throughput of Sending Bits		1	
20	Overall delay to detect a trusted vehicle			1	40	Throughput of Forwarding Packet			1

Table 3. LIST OF RESEACH PARAMETERS AND THEIR CATEGORIZATION

We have also reviewed research studies based on the type of urban scenarios used while applying research frameworks. Table. IV shows that different types of urban scenarios used in simulations of research studies. The urban scenario means the area where VANET is implemented on road. The areas can be of a city/urban, Highway or rural nature. The data is presented in Fig. 4 and Fig. 5. It shows that 61% of the surveyed studies did not specify the type of urban scenario used in the simulation while 26% of the studies used one scenario exactly. It also shows that 13% of the studies specified more than one scenario.

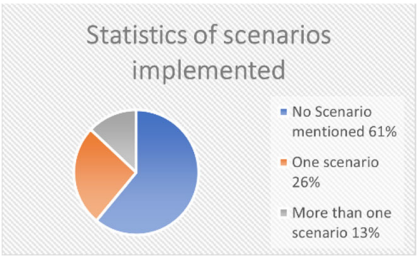

Fig 4. Statistics of scenarios implemented

Among the surveyed studies that specified one or more scenario for the simulation, Fig. 5 shows that the "Highway" scenario is the most used with a percentage of 44%. After this city scenario is 22% and rural scenario is used in 11% of the studies.

Table 4. FRAMEWORKS OF APPLICATION ENVIRONMENTS

Ref	Type of Evaluation		Simulation Software	Type of urban scenario		
	Simulation	Practical		Rural	High way	City/ Urban
[1]	✓		MATLAB			
[2]	✓		NetSim			
[3]	✓		MIRACL	✓		✓
[4]	✓		ONE		✓	
[5]	✓		NS-2			
[6]	✓		NS-2			
[7]	✓		NS-2			
[8]	✓		OMNET++		✓	✓
[9]	✓		Qualnet			
[10]	✓		Vanet-sim		✓	
[11]	✓		-			
[12]	✓		-			
[13]	✓		NS-2		✓	✓
[14]	✓		NS-2			
[15]	✓		QualNet			
[16]	✓		NS-2		✓	
[17]	✓		NS-2			✓

[18]	✓		NS-2			
[19]	✓		NS-2			
[20]	✓		VanetMobi Sim/ NS-2		✓	
[21]	✓		NS-2			
[22]	✓		NS-2			
[23]	✓		Java custom simulator			✓

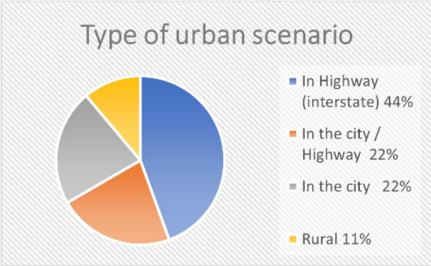

Figure 5. Types of urban scenarios

4. Conclusion and future work

This study focused on the identification of performance evaluation parameters for VANET security frameworks. This is done by surveying many research studies in this context, analyzing them and categorizing them based on nature of parameter evaluation (security-related, network-related, or general). Many survey studies are analyzed as part of literature re-view, most of them either focused on some specific perspective of the surveyed frameworks or had their results presented in a theoretical way instead of identification of any evaluation criteria. In addition to this, some practical information is also extracted to help future researchers. Some widely used simulators are identified alongwith implementation scenarios. All these pieces of practical information are presented in statistical way to direct future researchers to important implementation techniques and scenarios that can be used to evaluate proposed VANET security frameworks.

One of the most envisioned future development tracks for this research is to go into further analysis of the resulting parameters from this research study. The analysis shall be directed towards identification of the measurement methods and thresholds of the parameters to reveal a more detailed technique for evaluation of future proposed VANET security frameworks.

Acknowledgement

This work was supported by the Deputyship for Research and Innovation, Ministry of Education, Saudi Arabia, under Grant UQU-IF-P2-20-001.

References

[1] Avleen Kaur Malhi, and Shalini Batra, (2016) "Genetic-based framework for prevention of masquerade and DDoS attacks in vehicular ad-hoc net-works," Journal of Security and Communication Networks, vol. 9, no. 15, pp.2612-2626.

[2] B. K. Pattanayak, (2019) "Design and Development of Secured Framework for Efficient Routing in Vehicular Ad-Hoc Network" International Journal of Business Data Communications and Networking, Vol.15, pp. 55-72.

[3] Malhi, A., Batra, S. (2016). Privacy-preserving authentication framework using bloom filter for secure vehicular communications. International Journal of Information Security, 15(4), 433-453.

[4] Song J., He C., Yang F., Zhang H., (2016) "A privacy-preserving distance-based incentive scheme in opportunistic VANETs Security and Communication Networks" vol.9, pp- 2789-2801.

[5] Bharati S; Sindhankeri, Shraddha K. (2017), "A Multi Constrained Qos Routing Algorithm for Vehicular Adhoc Networks". International Journal of Advanced Research in Computer Science, [S.l.], v. 8, n. 7, p. 736-740.

[6] Tahani Gazdar, Abdelfettah Belghith, Ahmad AlMogren, (2017) "DTCF: A distributed trust computing framework for vehicular ad hoc networks", KSII Transactions on Internet and Information Systems (TIIS).

[7] Gopikrishnan, S., Krishnaraj, C., and Kokilavani. K, (2018) "HAAC: Reinforcing VANET Security Using Ant Colony Optimization through Heuristic Approach", in International Journal of Vehicle Structures Systems, vol. 10, no. 1, pp. 345-351 (Impact factor: 0.25).

[8] J. Jenefa, E. A. Mary Anita, (2018) "Secure Vehicular Communication Using ID Based Signature Scheme". Wireless Personal Communications 98(1): 1383-1411.

[9] R. Pradweap , R. Hansdah, (2013) " A Novel RSU-Aided Hybrid Architecture for Anonymous Authentication (RAHAA) in VANET" , International Conference on Information Systems Security, ICISS 2013, LNCS 8303, pp. 314–328.

[10] I. Bhattacharya, S.Ghosh and D. Show, (2014) "An Efficient and Secured Routing Protocol for VANET" Proceedings of the 3rd International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA), vol. 2, pp. 775-783.

[11] Y. Wang, J. Hu, X. Li and Z. Feng (2019) "An Efficient Mutual Authentication Framework with Conditional Privacy Protection in VANET" Collaborative Computing: Networking, Applications and worksharing, pp. 799-815.

[12] M. Kadam, S. Limkar (2013) "Detection and Mitigation of Misbehaving Vehicle from VANET" ICT and Critical Infrastructure: Proceedings of the 48th Annual Convention of CSI, Vol. 1, pp. 267-276.

[13] G. Kumaresan, T. Adiline Macriga (2016) "Group Key Authentication scheme for Vanet intrusion detection (GKAVIN)" Wireless Networks, vol. 23, pp. 935-945.

[14] M. Selvi, B. Ramakrishnan, (2019) "Lion optimization algorithm (LOA) based reliable emergency message broadcasting system in VANET" Soft Computing, pp. 1-18.

[15] M. Kaur, R. Rajni, and P. Singh (2012) " Performance Evaluation of V2VCommunication by Implementing Security Algorithm in VANET" Advances in Computing and Information Technology, vol. 176 , pp.757-763.

[16] G. B. Santhi, D. Sheela (2020) " Reliability refinement in VANET with hybrid jamming attacks using novel index based voting algorithm" Peer-to-Peer Networking and Applications, vol.13.

[17] M. Rath, B. K. Pattanayak (2017) "SCICS: A Soft Computing Based Intelligent Communication System in VANET" Communications in Computer and Information Science, vol,808, pp. 255-261.

[18] P. Manickam, K. Shankar, E. Perumal, M. Ilayaraja and K. S. Kumar (2019) "Secure Data Transmission Through Reliable Vehicles in

VANET Using Optimal Lightweight Cryptography" Cybersecurity and Secure Information Systems, pp. 193-204.

[19] D. Chuan (2012) "Towards a Trusted Vehicular Routing in VANET" Information Technology Convergence, Secure and Trust Computing, and Data Management, vol. 180, pp 103-117.

[20] R. Hussain, S. Kim and H. Oh (2016) "Traffic Information Dissemination System: Extending Cooperative Awareness Among Smart Vehicles with only Single-Hop Beacons in VANET" Wireless Personal Communications , vol. 88, pp. 151–172.

[21] R. Sugumar, A. Rengarajan and C. Jayakumar (2018) "Trust based authentication technique for cluster based vehicular ad hoc networks (VANET)" Wireless Networks, vol. 24, pp. 373-382.

[22] S. DasGupta, R. Chaki, and S. Choudhury (2013) "TruVAL: Trusted Vehicle Authentication Logic for VANET" Advances in Computing, Communication, and Control, vol. 361, pp. 309-322.

[23] H. Hu, R. Lu and Z. Zhang (2016) "VTrust: A Robust Trust Framework for Relay Selection in Hybrid Vehicular Communications" 2015 IEEE Global Communications Conference (GLOBECOM).

[24] Haerri, F. Filali, and C. Bonnet. (2006) "Performance comparison of AODV and OLSR in VANETs urban environments under realistic mobility patterns." Proceedings of the 5th IFIP mediterranean ad-hoc networking workshop.

[25] Khairnar, D. Pradhan, N. (2013) "Simulation Based Evaluation of Highway Road Scenario between DSRC/802.11p MAC Protocol and STDMA for Vehicle-to-Vehicle Communication" . Journal of Transportation Technologies, 3, 88-104

[26] Azees, M., Vijayakumar, P., Deborah, L,J. (2016) "Comprehensive survey on security services in vehiclear ad-hoc network". Intell. Transp. Syst. 10(6), 12.

[27] Al-Sultan, S., Al-Doori, M.M., Al-Bayatti, A.H. and Zedan, H. (2014) "A Comprehensive Survey on Vehicular Ad Hoc Network". Journal of Network and Computer Applications, 37, 380-392.

[28] Cheng X., Chen C., Zhang W., Yang Y. (2017) "5G-Enabled Cooperative Intelligent Vehicular (5GenCIV) Framework" IEEE Intell. Syst. ;32:53–59. doi: 10.1109/MIS.2017.53.

[29] Hasrouny H., Abed Ellatif S., Bassil C., Laouiti, A. (2017). "VANET Security Challenges and Solutions: A Survey" Vehicular Communications 7:7-20

[30] S. S. Kaushik, (2013) "Review of different aproaches for privacy" International Journal of Advanced Engineering and Technology, vol. 5, no. 2, pp. 356–363.

[31] M. Gonzalez-Martin, M. Sepulcre, R. Molina-Masegosa, and J. Gozalvez, (2019) "Analytical models of the performance of C-V2X mode 4 vehicular communications," IEEE Transactions on Vehicular Technology, vol. 68, no. 2, pp. 1155–1166.

[32] Molina-Masegosa R., Gozalvez, J. (2017). "TE-V for Sidelink 5G V2X Vehicular Communications: A New 5G Technology for Short-Range Vehicle-to-Everything Communications", IEEE Vehicular Technology Magazine 12(4):30-39

[33] S. Chen, J. Hu, Y. Shi, and L. Zhao, (2016) "LTE-V: a TD-LTE-based V2X solution for future vehicular network," IEEE Internet of Things Journal, vol. 3, no. 6, pp. 997–1005.

[34] J. M. de Fuentes, A. I. Gonzalez-Tablas, and A. Ribagorda, (2010) "Overview of Security Issues in Vehicular Ad Hoc Networks", Hershey, Derry Township, PA, USA.

[35] Jakubiak J., Koucheryavy Y. (2008) "State of the Art and Research Challenges for VANETs", 5th IEEE Consumer Communications and Networking Conference.

[36] A. Dhamgaye and N. Chavhan, (2013) "Survey on security challenges in VANET," International Journal of Computer Science, vol. 2, pp. 88–96.

[37] Y. L. Morgan, (2010) "Notes on DSRC WAVE standards suite: its architecture, design, and characteristics," IEEE Communications Surveys Tutorials, vol. 12, no. 4, pp. 504–518.

[38] Yousefi S., Mousavi M., Fathy M., (2006) "Vehicular ad hoc networks (VANETs): challenges and perspectives", 6th International Conference on ITS Telecommunications, pp 761-766.

[39] Z. Lu, G. Qu, and Z. Liu, (2019) "A survey on recent advances in vehicular network security, trust, and privacy," IEEE Transactions on Intelligent Transportation Systems, vol. 20, no. 2, pp. 760–776.

[40] Muhammad Sameer Sheikh, Jun Liang, (2019) "A Comprehensive Survey on VANET Security Services in Traffic Management System", Wireless Communications and Mobile Computing, Article ID 2423915, 23 pages.

[41] Muhammad Sameer Sheikh, Jun Liang, W. Wang, (2020)" Security and Privacy in Vehicular Ad Hoc Network and Vehicle Cloud Computing: A Survey", Wireless Communications and Mobile Computing, vol. 2020, Article ID 5129620, 25 pages.

[42] Sheikh, Liang, Wang,. (2019). A Survey of Security Services, Attacks, and Applications for Vehicular Ad Hoc Networks (VANETs). Sensors. 19. 3589. 10.3390/s19163589.

[43] Y. R. B. Al-Mayouf, M. Ismail, N. F. Abdullah, S. M. Al-Qaraawi and O. A. Mahdi (2016). "Survey On Vanet Technologies And Simulation Models" , ARPN Journal of Engineering and Applied Sciences, VOL. 11, NO. 15

[44] M. A. Elsadig, Y. A. Fadlalla (2016) . "VANETs security issues and challenges: A survey", Indian Journal of Science and Technology, Vol (9).

[45] A. khan, M. Ishtiaq, S. Anwar and M. A. Shah (2019). "A Survey on secure routing strategies in VANETs", 2019 25th International Conference on Automation and Computing (ICAC)

[46] Sajjad Akbar Mohammad, Asim Rasheed, Amir Qayyum (2011) "VANET architectures and protocol stacks: a survey" International Workshop on Communication Technologies for Vehicles, Page 95-105.

[47] Abir Mchergui, Tarek Moulahi, Bechir Alaya, Salem Nasri (2017) . "A survey and comparative study of QoS aware broadcasting techniques in VANET", Telecommunication Systems, Vol (66), Pages 253-281.

[48] C. Chen, Y. Chen, C. Lee and Y. Deng (2018). "A Survey of Authentication Protocols in VANET Advances on Broadband and Wireless Computing, Communication and Applications (pp.572-577)

[49] MA Razzaque, Ahmad Salehi, Seyed M Cheraghi (2013). "Security and Privacy in Vehicular Ad-Hoc Networks: Survey and the Road Ahead", Wireless Networks and Security, SCT, pp. 107–132.

[50] Irshad Ahmed Sumra, Halabi Bin Hasbullah, Jamalul-lail Bin AbManan (2015). "Attacks on security goals (confidentiality, integrity, availability) in VANET: a survey", Vehicular Ad-Hoc Networks for Smart Cities, page 51-61.

[51] V. Vijayalakshmi ; M. Sathya ; S Saranya ; C. Selvaroopini (2015). "Survey on various mechanisms for secure and efficient VANET communication", International Conference on Information Communication and Embedded Systems.

[52] Aakash Luckshetty, Sindhu Dontal, Shrikant Tangade, Sunilkumar S Manvi (2016). "A survey: comparative study of applications, attacks, security and privacy in VANETs" International Conference on Communication and Signal Processing, April 6-8.

[53] N. S. Patel, S. Singh. (2016) "A Survey on Techniques for Collision Prevention in VANET", International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)

[54] Fengzhong Qu ; Zhihui Wu ; Fei-Yue Wang ; Woong Cho (2015). "A Security and Privacy Review of VANETs", IEEE Transactions o Intelligent Transportation Systems (Volume): 16 , Issue: 6.

[55] M. Kim, (2018)" A Survey of Vehicular Ad-Hoc Network Security", Mobile and Wireless Technologies 2017, Volume 425.

[56] online:https://internetofthingsagenda.techtarget.com /definition/Cellular-Vehicle-to-Everything-C-V2X

Emad Felemban is a full professor in Computer Engineering Department Umm AlQura University, Makkah, Saudi Arabia. He earned his M.Sc. and Ph.D. from Ohio State University in 2003 and 2009, respectively. His research interests include wireless sensor networks algorithm and protocols, Smartcity applications, and smart antennas. Currently, Dr. Felemban is leading the transportation and crowd management center of research excellence in Umm Al-Qura University working on cutting edge research.

***S*alem M. Albogamind** received the B.E., M. E. degrees from Umm Al-Qura University. He is working as a researcher in Umm Al-Qura. His current research interests are Internet of Things, Wireless Sensor Networks, Vehicular Network.

Atif Naseer obtained his BS degree in Software Engineering from UET Taxila, Pakistan and MS degree in Software Engineering from National University of Sciences and Technology, Pakistan. He is acadamecian by profession and is currently serving as lecturer and researcher in Science and Technology Unit at Umm-al-Qura University, Makkah, Kingdom of Saudi Arabia. He has been attached with academia for over 8 years and has served as permanent faculty in many prestigious universities. His area of specialization are Software Engineering, Wireless Sensor Networks, Wireless Mesh Networks, Simulation and Modeling, Big Data Analysis, Geographic Information Systems. Contact him at the Science and Technology Unit, Umm-al-Qura University, Makkah Saudi Arabia; anahmed@uqu.edu.sa.

HASSAN H. SINKY received the M.S. and Ph.D. degrees from Oregon State University, USA. Since 2017, he has been an Assistant Professor with the College of Computer and Information Systems, Umm Al-Qura University, Saudi Arabia. He specializes in large urban wireless communication networks, content-delivery and content-centric networks, quality of service and quality of experience methods, cross-layer assisted multi-path TCP, and seamless handoffs in wireless mobile scenarios.