EasyChair Preprint

№ 10194

Concerns and Difficulties Associated with Vehicular Ad Hoc Networks (VANET)

Ahmad Salem

May 17, 2023

Concerns and Difficulties Associated with Vehicular Ad Hoc Networks (VANET)

Ahmad AA Salem

Abstract

While there is always room for improvement in network defences against adversaries and assaults, the emphasis of current research is mostly on the security of Vehicular Ad Hoc Networks in order to provide drivers and manufacturers with both life safety and entertainment (VANET). This essay will focus on the security and privacy aspects of VANET networks, which are critical to their reliability.

Additionally, we looked at possible solutions to these concerns and critiqued them while also putting out our own ideas for how to fix some of the most pressing ones. Many issues have been addressed in this research, including VANET's difficulties.

1. BACKGROUND

Vehicular Networks is going to be the most important actor in this activity, with the goal of enabling road safety, efficient driving, and entertainment. The attempts to create driving circumstances that are safer, more pleasant, and more efficient have begun. The world we live in is currently in the midst of a war, and the front lines of this conflict are the roads. Each year, it is estimated that approximately 1.2 million people are killed on the world's roadways [1, 2, 3, 4, and 5]. About forty times as many people are injured, and this is not to mention the fact that traffic congestion results in a significant loss of both time and fuel [6, 7, 8, 9, 10, 11, 12, 13, and 14].

This implies that no matter where a node in a VANET moves within the network's coverage area, it will stay linked to the rest of the network through a mobile ad hoc network (MANET). It is possible for vehicles, roadside equipment, or even another VANET node to connect with any other nodes in a VANET in a single hop or several hops (RSU) [15, 16].

Engineers from Delphi Delco Electronics System and IBM Corporation came up with the notion of a network vehicle in 1998, with the goal of providing a wide range of applications. Because of advancements in wireless communication technology, individuals from many walks of life are interested in a networked car [17, 18, 19, 20].

An increasing number of ground-breaking projects have been launched in recent years with the objective of creating vehicular networks and bringing about the long-awaited networking of automobiles. As part of a joint effort by DaimlerChrysler, BMW, Volkswagen, the Fraunhofer Institute for Open Communication Systems (IOCS), NEC Deutschland GmbH, and Siemens AG, NOW was launched in 2004 [21, 22, 23]. Uses IEEE 802.11 wireless access, and its primary aims are to address issues related to data security and protocols for car-to-car communications.

Automotive manufacturers from throughout Europe came together to form the Car2Car Communication Consortium. Developing a European industry standard for car-to-car communications that is compatible with all manufacturers is the goal of this group. An additional European scheme called FleetNet [16] was implemented in the period 2000-2003. This ad hoc research was dominated by efforts to standardize MANET protocols, and this MANET research focused on the network layer [24, 25, 26, 27, 28, 29, 30]. As part of the European Commission's objective of lowering the incidence of automobile accidents by half by 2010, a new research initiative has been launched in this area. The final challenge was to overcome the issue of reaching nodes that were not immediately within radio range by employing neighbors as forwarders [31, 32].

Dedicated Short-Range Communications (DSRC) is the name given to the radio used for communication by the Federal Communications Commission (FCC) in 1999 [33]. With a frequency range of 5.9 GHz to 75 MHz, the band was designed for use in North American ITS applications only.

Message integrity and source authentication are terms used to describe how a VANET's security measures guarantee that the information received is accurate, that the source is who he claims to be, that the node delivering the message cannot be traced, and that the system as a whole is resilient [34, 35, 36, 37, 38].

Our analysis of VANET Attack and Attackers, which takes place in the second part of our paper, serves to illustrate the problems that VANET is now facing. This section focuses on VANET security considerations, such as mobility and privacy, which are considered the most critical. In the fourth section, we discuss the security requirements that must be in place before a security system may be put in place. It's time to wrap things up with a look at what we've done so far, and what's still needed to develop a secure system [39, 40, 41].

2. HOW VEHICULAR NETWORKS WORK

DSRC (5.9 GHz) radio transmissions, with a range of up to one kilometre, may be used by each automobile to communicate with other cars. As this is an ad hoc connection, nodes may move freely without the need for wires. Road Side Units (RSU) are the routers used, and the Vehicular Networks System consists of several nodes. Around 750 million cars are on the road right now [42, 43].

The acronym "on board unit" (abbreviated "OBU") appears on every vehicle. To connect the automobile to the RSU, this gadget makes use of DSRC radios. Each vehicle has a "tamper proof device," which stands for "tamper proof device." This device keeps track of every detail about the vehicle, from the keys to the driver's identity to the trip statistics, speed, and route [44, 45, 46].

3. SECURITY ISSUES OF VEHECULAR NETWORKS

Following are some of the attacks against VANET that are discussed:

Attainments and Threats of Assault

In this project, physical security is not an issue, thus we will focus on attacks on the message rather than on the vehicle.

1) An attack against the service provider

Vehicle resources or the Vehicular Network communication channel may be taken over by an attacker in order to prevent vital information from being sent. Additionally, the driver's safety might be compromised if it is compelled to depend on the app's information.

An evildoer, for example, may instigate an accident and then use a denial-of-service assault to prevent the warning from reaching the approaching vehicles [47, 48].

Using multiple radio transceivers operating in separate frequency bands may be a viable solution to the Denial-of-Service (DoS) problem, according to authors [49], but even this approach will necessitate the addition of new and more equipment to the vehicles, which will necessitate the expenditure of additional funds and space in the vehicle.

DSRC, UTRA-TDD, or even Bluetooth for very short ranges may be used in the event that one of them (typically DSRC) is unavailable, as the developers of [50] explain in their solution.

2), an attacker purposely loses packets from the network, which may include critical information for the receiver, and the attacker suppresses these packets and may use them again at a later date[51].

An assailant of this kind would want to conceal accidents involving his vehicle from registration and insurance organizations and to prevent accident reports from being submitted to roadside access points [52].

3) Congestion notices may be hidden and then deployed at a later time, so that cars miss the warning and are forced to wait.

Fabrication Attack: An attacker may use this attack to send false information into the network, either incorrectly or pretending to be another person.

Messages, warnings, certificates, and identities are all forged in this assault.

4) Data Modification Attack: This attack happens when an attacker makes changes to data that has already been collected. By delaying, replaying, or otherwise altering the actual entry of the data transmitted, it is possible to manipulate the flow of data.

The message that tells other cars that the current route is clear, while in reality it is jammed, may be altered by an attacker [53].

5) Replay of the attack

Basically, an attacker replicates a previously transmitted message in an attempt to take advantage of the message's state during transit [54].

Basic 802.11 security does not provide any defense against replay attacks. It does not have time stamps or sequence numbers. Key reuse means that stored messages may be replayed with the same key and used to insert fraudulent messages into the system. Instead than just encrypting data, each packet must be authenticated. Packets must have timestamps.

Assaults like this one are designed to confuse law enforcement in hit-and-run scenarios and maybe prevent vehicle identification [55].

6) An assault by Sybil Assault

One way to trick other drivers into taking another route is to use a slew of pseudonymous automobiles and pretend there are over a hundred of them on the road [5] or to act as though there are.

What determines the efficacy of a Sybil attack depends on how easily and cheaply identities can be created, how much input the system accepts from entities that don't have a trustworthy chain of trust, and if the system treats all entities equally.

Using the example of a hundred cars, an attacker may convince other drivers on the road that traffic is congested and that they should take another route to keep the road free of obstructions of their own making.

CONSIDERATIONS

A Driver Who Is Selfish

All cars in the vehicular network must first be trusted to obey the protocols provided by the application, which is the main notion underlying trust in the network's automobiles. It's also true that certain drivers will go to great lengths to maximize their own profit from the network, regardless of the cost to the system.

In order to clear the road, a selfish motorist may tell other drivers to take a different route because of traffic.

Apps on the vehicular network may be used by malicious attackers to inflict damage. [56] and [57] In many cases, these attackers have specific targets in mind and have access to network resources.

Before detonating a bomb, a terrorist, for example, may issue a deceleration warning in order to generate traffic gridlock.

People who play pranks

[5] Hackers and bored people searching for vulnerabilities are two examples.

Consider the possibility that someone can get one automobile to slow down while giving the driver of the one behind it instructions to speed up.

Problems with vehicular networks are the third issue addressed in this chapter.

a person's ability to move about

Since each node in an Ad Hoc Network is mobile, it is possible for it to move across the coverage region, but this mobility is still restricted. As each car travels in its own way, vehicles in Vehicular Ad Hoc Networks nodes communicate with other vehicles they may have never met before, and this connection lasts just a few seconds. Achieving movement is difficult because of this. Many research have been undertaken in an attempt to remedy this problem [5, 9].

The degree of fluctuation in price.

If the connection is broken, it is possible that the two nodes will never connect again. Passing through the coverage area and connecting with other cars will lose these connections since each automobile has a high mobility and may go in the other direction [1],[5].

To secure VC, long-lived passwords will be required for personal interactions between a user's device and a hot spot, which is troublesome for vehicle networks.

Thirdly, authentication vs. privacy.

Authentication in Vehicular Ad Hoc Networks is important to prevent the Sybil Attack [8], which has already been mentioned.

In order to avoid this problem, we may supply each automobile with its own identifier. However, the majority of drivers will not be able to use this method since they want to keep their personal information private [1],[5].

4) Privacy vs. Responsibility

Data collected as a result of a collision cannot be withheld under any circumstances. However, personal information should not be misused and each motorist should have the opportunity to keep his or her information private from others (Identity, Driving Path, Account Number for toll Collector etc.).

Expandability of the Network

Another issue arises when we consider the fact that there is no global authority that governs the standards for this network. For example DSRC in North America differs from those in Europe; the standards for GM vehicles differ from those of BMW; and the standards for Bluetooth differ from those for DSRC in North America.

Bootstrap

If we communicate with the current fleet of automobiles, we must expect that only a small number of cars would get our message. In the future, we must work to increase the number of cars equipped with DSRC radios so that commercial enterprises will be more likely to invest in this technology [5].

3. REQUIREMENTS FOR SECURITY

1) Authentication

An authenticated message in VC ensures the communication's origin and enables vehicle-level control. Vehicles will allocate their Private Key and Certificate to each communication in order to do this. Upon receiving the message, the vehicle checks for the key and certificate; after this is done, the receiver confirms [1], [5].

ECC (Elliptic Curve Cryptography), the efficient public key cryptosystem, may be used to reduce the cost of signing each message, or we can sign the key just for the most important communications.

2) Accessibility

Sensor Networks and even Ad Hoc Networks will be required to provide real-time responses for many applications, and a delay of even a few seconds might make a communication useless, with fatal results[1][5].

A denial-of-service attack may be launched against a system that is trying to meet real-time demands. An application layer failure makes this problem much worse since the only way to recover from incorrect transmission is to save partial messages and hope that they will be completed in a subsequent transfer.

3) The principle of non-refutation

A non-repudiation can help identify the perpetrators even after an assault has happened [5, 8]. As a consequence, cheaters are unable to argue their innocence.

The TPD will save all relevant information on a vehicle, including its route, speed, time, and any violations, which may be accessed by any official with proper authorization.

Fourth, drivers' information such as their genuine identities, travel routes and speeds are protected from unwanted observers by the system's privacy features.

This may be done by using anonymous keys that are only used once and expire after usage [1], all of which will be stored in the TPD and reloaded each time a vehicle undergoes an official inspection [5]. [1]

The genuine identity of the motorist is concealed behind an ELP (Electronic License Plate). Every new automobile comes with a license plate that can be read using RFID technology, which is why it's required in the manufacturing process.

Getting a court order to find out the actual identity of a certain automobile ELP may be done by the police or any other authority.

Limitations in terms of time

A real-time response is required in some circumstances while driving at high speeds, otherwise the results might be devastating [5].

The future DSRC standard, which is based on an extension of IEEE 802.11 technology, is the basis for current car network plans.

Integrity is the sixth quality.

In order to prevent attackers from tampering with the integrity of communications, all messages should be authenticated [1].

Seventh: Confidentiality

Communications between drivers must be encrypted so that no one else may get their hands on the driver's information [1].

THE LATEST ADVANCEMENTS IN SOLUTIONS

An abundance of VANET security solutions and publications have been published to address the problems listed above. VPKI (Vehicular Public Key Infrastructure) was advocated as a solution by the authors in [1] and [7]. Each node has a public/private key. With its own private key and the Certificate Authority's (CA) certificate, a vehicle signs a safety message.

V's certificate will be used by the message's receivers to get V's public key, which they will then use to authenticate V's signature. If the CA's public key [12] is known by the recipient, this solution may be used [3, 5, 10, and 11].

When a vehicle joins the group area, the group public key and the vehicle session key for each vehicle that belongs to the group must be modified and sent. This is a fundamental shortcoming of the group signature suggested by the developers of [20]. Additionally, the VANET's mobility hinders the network from building a stable group, because the sig changes often and the group members are always moving about.

The use of CA, which requires infrastructure, has also been suggested as an alternative. A large number of CAs are needed to govern VANET. Until date, there has been no actual authority in the VANET realm to oversee its affairs.. To manage all certificate activities, including issuance, renewal, and revocation, the CA has been recommended by many researchers, including [4, 7, 10, 11, 12, 13, 14]. The CA also has to be in charge of producing and renewing certificates, as well as maintaining and broadcasting CRLs.

Cars would sign each communication with their private key and attach a certificate to ensure that the messages were valid. ECC has been recommended as a technique to decrease this cost, whereas writers in [3] suggested a different approach, employing short-term and long-term certificates for the keys. A long-term certificate is used to authenticate the user, whereas a short-term certificate is used to exchange data. In order to verify the truth of safety messages, they are not encrypted. A source can sign and send a message without encryption using its certificate; other nodes receiving the message can validate it using the certificate and signature and may forward it without modification if the message is valid; any adversary can inject false information as a safety message because it doesn't need

to be encrypted; it can also steal the certificate from any other safety message and send an unencrypted message containing false information along with the certificate.

Using VPKI in VANET has a number of drawbacks, including the need to invalidate an attacker's certificate. To revoke an expired certificate and inform other cars, the Certificate Revocation solution was provided in [1]. While CRLs (Certificate Revocation Lists) are the most common way to revoke a certificate, this method has certain drawbacks: In the first place, CRLs might take a long time due of the huge number of automobiles and their rapid movement. Secondly, certificates have a finite life span, and there is no CRL infrastructure in place. Some revocation protocols, such as RTPD (Revocation Protocol of the Tamper-Proof Device), RCCRL (Revocation Protocol Using Compressed Certificate Revocation Lists), and DRP (Device Revocation Protocol) are also mentioned (Distributed Revocation Protocol), This method relies on monitoring, so every vehicle must monitor and detect all the vehicles around it; however, this method did not consider the reputation system, so it is possible for a large number of adversary vehicles to make an accusation, resulting in an unnecessary revocation. This method is also discussed in detail in [4], and has been proposed in [11].

Using a set of anonymous keys that change often (every few minutes), the authors of [1] propose a method for preserving privacy while driving. Only one key may be used at a time; each key expires after one usage. Pre-programmed keys stay in the TPD for a long length of time; each key must be authorized by the issuing CA and has a finite life expectancy (e.g., a specific week of the year). The drawback of this method is that the keys must be kept somewhere safe in order to determine the ELP's genuine identity.

According to the authors of [3,] IP version 6 has been suggested for use in automotive networks since cars may modify their IP addresses and use random MAC addresses to maintain security. If cars could change their IP addresses, this would make it impossible for the government to follow them.

This might also contribute to inefficiencies in the usage of addresses, since the old address cannot be instantly utilized when a new one is assigned. Delayed packets are lost when the car's IP address changes, resulting in unnecessary retransmissions.

As a possible solution, the authors of [5] suggested needing frequent inspections, which are required in most US states once a year for all vehicles. In addition to the standard maintenance, this yearly trip to the mechanic provides unique chances for security upkeep.

BRIEF RESUME AND PROSPECTIVE WORK

To attack the network with destructive assaults, attackers are going to exploit Vehicular Ad Hoc Networks (VAN) technologies. With the help of this article, we were able to give an in-depth look at present VANET security issues, as well as criticism of existing solutions. We also came up with a few new ideas for improving VANET security, and we plan to test them in simulations in the future.

REFERENCES

1. Hassan, M.A., Ghassan Samara, Mohammad Abu Fadda, 2022. IoT Forensic Frameworks (DFIF, IoTDOTS, FSAIoT): A Comprehensive Study, *International Journal of Advances in Soft Computing & Its Applications, 14(1).*
2. Ghassan Samara, Hassan, M.A. And Al-Okour, M.U.N.I.R., 2022. Energy Balancing Algorithm For Wireless Sensor Network. *Journal Of Theoretical And Applied Information Technology, 100(4).*
3. Ghassan Samara, 2021. Lane prediction optimization in VANET. *Egyptian Informatics Journal*, *22*(4), pp.411-416.
4. Ghassan Samara, Hassan, M.A. and Zayed, Y., 2021. An Intelligent Vice Cluster Head Election Protocol in WSN. *Int. J. Advance Soft Compu. Appl*, *13*(3).
5. AlShourbaji, I., Ghassan Samara, abu Munshar, H., Zogaan, W.A. and Reegu, F.A., 2021. Early detection of skin cancer using deep learning approach. *Elementary Education Online*, *20*(5), pp.3880-3884.
6. Ghassan Samara, Samara, G., 2020. Intelligent reputation system for safety messages in VANET. *IAES International Journal of Artificial Intelligence*, *9*(3), p.439.
7. Ghassan Samara, *2020.* Optimal Number of Cluster Heads in Wireless Sensors Networks Based on LEACH, *International Journal of Advanced Trends in Computer Science and Engineering (IJATCSE), 9(1).*
8. Ghassan Samara, *2020.* Energy-Efficiency Routing algorithms in Wireless Sensor Networks: a Survey, *International Journal Of Scientific & Technology Research, 9(1).*

9. Ghassan Samara, 2019. An Improved CF-MAC Protocol for VANET, *the International Journal of Electrical and Computer Engineering (IJECE) 9(4), p. 2668.*

10. Ghassan Samara, Mohammad Khawaldeh, 2019. Efficient Energy, Cost Reduction, and QoS based routing protocol for Wireless Sensor Networks, *the International Journal of Electrical and Computer Engineering (IJECE), 9(1).*

11. Ghassan Samara, Mohammad Khawaldeh, 2018. Aware-Routing Protocol using Best First Search Algorithm in Wireless Sensor, *The International Arab Journal of Information Technology, 15(3A),p.592.*

12. Ghassan Samara, 2018. An Efficient Collision Free Protocol for VANET, *International Journal of Computer Applications (IJCA) 180(16), p.30.*

13. Ghassan Samara, 2018. An Intelligent Routing Protocol in VANET, *the International Journal of Ad Hoc and Ubiquitous Computing (IJAHUC), Inderscience Publishers 29(1), p.77.*

14. Tareq Alhmiedat, Ghassan Samara, 2017. A Low Cost ZigBee Sensor Network Architecture for Indoor Air Quality Monitoring, *International Journal of Computer Science and Information Security, 15 (1).*

15. Ghassan Samara, 2017. A Practical Approach for Detecting Logical Error in Object Oriented Environment, *World of Computer Science and Information Technology Journal (WCSIT), 7(2), p.10.*

16. Emran Hassan Al Saleh, Ghassan Samara, 2015. Mobile Station-Controlled Handover Scheme in Mobile WiMAX: Case Study, *International Journal of Computer Applications 127(8), p.12.*

17. Abla Hussein, Ghassan Samara, 2015. Coordinator Location Effects in AODV Routing Protocol in ZigBee Mesh Network, *International Journal of Computer Applications 127(8), p.1.*

18. Maimuna Khatari, Ghassan Samara, 2015. Congestion Control Approach based on Effective Random Early Detection and Fuzzy Logic, *MAGNT Research Report ,3 (8). P.180.*

19. Abla Hussein, Ghassan Samara, 2015. Mathematical Modeling and Analysis of ZigBee Node Battery Characteristics and Operation, *MAGNT Research Report ,3 (6). P.99*.

20. Khalid Abedel-fatah Alkheder, Ala Ahmad Al-Shoubaki, Ghassan Samara, 2015. "The Development of Wireless Communication Systems from Zero Generation to Fifth Generation - A survey, *International Journal of Sciences & Applied Research, IJSAR, 2(5), p.41*.

21. Asem M. Uweineh, Ghassan Samara, 2015. Improved Routing Performance in Sensor Networks Using Virtual Coordinates (Survey), *International Journal of Sciences & Applied Research, IJSAR, 2(5), p.35.*

22. Emran Hassan Mohammed Al Saleh, Ghassan Samara, 2015. TCP and UDP QoS Characteristics on Multiple Mobile Wireless LAN, *International Journal of Sciences & Applied Research, IJSAR, 2(4), p.64*.

23. Yousef Al-Raba'nah, Ghassan Samara, 2015. Security Issues in Vehicular Ad Hoc Networks (VANET): a survey, *International Journal of Sciences & Applied Research (IJSAR), 2(4), p.50.*

24. Ghassan Samara, Mohammad Rasmi, 2015. Deploying an Efficient Safety System for VANET, *The World of Computer Science and Information Technology Journal (WSCIT). 5(3), p.41*.

25. Amneh Alamleh, Ghassan Samara, 2015. New Strategy for Cache Replacement in Manets, *Global Journal of Advanced Research (GJAR), 2 (1), p.230.*

26. Ghassan Samara, Tareq Alhmiedat, 2014. Intelligent Emergency Message Broadcasting in VANET Using PSO, *World of Computer Science and Information Technology Journal (WCSIT), 4 (7) p.90.*

27. Amer O. Abu Salem, Ghassan Samara, Tareq Alhmiedat, 2013. Performance Analysis of Dynamic Source Routing Protocol, *Journal of Emerging Trends in Computing and Information Sciences, 5 (2), p.97.*

28. Ghassan Samara, Amer O Abu Salem, Tareq Alhmiedat, 2013. Power Control Protocols in VANET, *European Journal of Scientific Research, 111(4), p.571*.

29. Ghassan Samara, Tareq Alhmiedat, Amer O. Abu Salem, 2013. Dynamic Safety Message Power Control in VANET Using PSO, *World of Computer Science and Information Technology Journal (WCSIT), 3(10) p.176.*

30. Amer O Abu Salem, Tareq Alhmiedat, Ghassan Samara, 2013. Cache Discovery Policies of MANET, *World of Computer Science and Information Technology Journal (WCSIT), 3(8), p.135.*

31. TA Alhmiedat, A Abutaleb, Ghassan Samara, 2013. A Prototype Navigation System for Guiding Blind People Indoors using NXT Mindstorms", *International Journal of Online Engineering (iJOE), 9(5), p.52.*

32. Ghassan Samara, Wafaa Alsalihy, R Sures, 2013. Survey on security challenges in VANET, *IJCSN International Journal of Computer Science and Network, 2(1).*

33. Tareq Alhmiedat, Ghassan Samara, Amer O Abu Salem, 2013. An Indoor Fingerprinting Localization Approach for ZigBee Wireless Sensor Networks", *European Journal of Scientific Research 105(2), p.190.*

34. Ghassan Samara, 2012. Certificate Revocation Management in VANET, *International Journal of Cyber-Security and Digital Forensics (IJCSDF), 1(2), p . 115.*

35. Ghassan Samara, Wafaa Alsalihy, 2012. Message Broadcasting Protocols in VANET, *Information Technology Journal, 11, p.1235.*

36. Ghassan Samara, Wafaa Alsalihy, Sureswaran Ramadass, 2011. Increase Emergency Message Reception in VANET, *Journal of Applied Sciences, 11(14), p.2606.*

37. Ghassan Samara, Wafaa Alsalihy, Sureswaran Ramadass, 2011. Increasing Network Visibility Using Coded Repitition Beacon Piggybacking, *World Applied Sciences Journal (WASJ), 13(1), p.100.*

38. Ghassan Samara, Sureswaran Ramadas, Wafaa Alsalihy, 2010. Safety Message Power Transmission Control for VANET", *Journal of Computer Science, 6(10), p.1027.*

39. Ghassan Samara, Wafaa Alsalihy, Sureswaran Ramadass, 2010. A broadcast scheme in dense VANETs, *Journal of Applied Sciences, 11(14), p.3960.*

40. Ghassan Samara, Wafaa Alsalihy, R. Suress, 2010. Design of Simple and Efficient Revocation List Distribution in Urban areas for VANETs", *International Journal of Computer Science and Information Security (IJCSIS), 11(1), p.151*.

41. Ghassan Samara, Hussein, M. and Khaled, A.Q., 2021, December. Alarm System at street junctions (ASSJ) to avoid accidents Using VANET system. In *2021 Global Congress on Electrical Engineering (GC-ElecEng)* (pp. 37-41). IEEE.

42. Al-Mousa, M.R., Sweerky, N.A., Ghassan Samara,,Alghanim, M., Hussein, A.S.I. and Qadoumi, B., 2021, December. General Countermeasures of Anti-Forensics Categories. In *2021 Global Congress on Electrical Engineering (GC-ElecEng)* (pp. 5-10). IEEE.

43. Ghassan Samara, Quaddoura, R., Al-Shalout, M.I., Khaled, A.Q. and Al Besani, G., 2021, Internet of Things Protection and Encryption: A Survey. In 2021 22nd International Arab Conference on Information Technology (ACIT) (pp. 1-7). IEEE.

44. Ghassan Samara, Hussein, A., Matarneh, I.A., Alrefai, M. and Al-Safarini, M.Y., 2021, Internet of Robotic Things: Current Technologies and Applications. In *2021 22nd International Arab Conference on Information Technology (ACIT)* (pp. 1-6). IEEE.

45. Quaddoura, R. and Ghassan Samara, 2021, Scheduling UET-UCT DAGs of Depth Two on Two Processors. In *2021 22nd International Arab Conference on Information Technology (ACIT)* (pp. 1-6). IEEE.

46. Hussain, I., Ghassan Samara, Ullah, I. and Khan, N., 2021, Encryption for End-User Privacy: A Cyber-Secure Smart Energy Management System. In *2021 22nd International Arab Conference on Information Technology (ACIT)* (pp. 1-6). IEEE.

47. Ghassan Samara, Rasmi, M., Sweerky, N.A., Al Daoud, E. and Salem, A.A., 2021, December. Improving VANET's Performance by Incorporated Fog-

Cloud Layer (FCL). In *2021 22nd International Arab Conference on Information Technology (ACIT)* (pp. 1-5). IEEE.

48. Ghassan Samara, Wireless Sensor Network MAC Energy-efficiency Protocols: A Survey. In *2020 21st International Arab Conference on Information Technology (ACIT)* (pp. 1-5). IEEE.

49. Ghassan Samara, Mohammad Khawaldeh, Aware-Routing Protocol using Best First Search Algorithm in Wireless Sensor Networks, *The 18th International Arab Conference on Information Technology (ACIT'2017).*

50. Ghassan Samara, Khiri M Blaou, Wireless Sensor Networks Hierarchical Protocols, *The 8th International Conference on Information Technology (ICIT 2017).*

51. ABM Shamsuzzaman Sadi, Towfique Anam, Mohamed Abdirazak, Abdillahi Hasan Adnan, Sazid Zaman Khan, Mohamed Mahmudur Rahman, Ghassan Samara, Applying ontological modeling on Quranic" nature" domain, *2016 7th International Conference on Information and Communication Systems (ICICS), 151-155.*

52. Arwa Husien, Ghassan Samara, Application Layer Protocols to Protect Electronic Mail from Security Threads, *in Proceeding of The 7th International Conference on Information Technology, ICIT 2015, 270.274*.

53. Ala'a H. Makableh, Ghassan Samara, Impact of Node Clustering on Power Consumption in WSN, A Comparative Study, *in Proceeding of The 7th International Conference on Information Technology, ICIT 2015, 266.269*.

54. Ghassan Samara, Wafaa Alsalihy, A New Security Mechanism for Vehicular Communication Networks, *Proceeding of the International Conference on Cyber Security, CyberWarfare and Digital Forensic (CyberSec2012), Kuala Lumpur, Malaysia. P. 18 – 22.*

55. Ghassan Samara, Wafaa Alsalihy, R. Suress, Security Analysis of Vehicular Ad Hoc Networks (VANET), *Proceeding of the 2nd International Conference on Network Applications (NETAPPS'10), Protocols and Services 2010, UUM, Malaysia*.

56. Ghassan Samara, Wafaa Alsalihy, R. Suress, Security Issues and Challenges of Vehicular Ad Hoc Network, *Proceeding of 4th International Conference on New Trends in Information Science and Service Science (NISS 2010), Gyeongju, South Korea, May 11, 2010.*

57. Ghassan Samara, Wafaa Alsalihy, R. Suress, Efficient Certificate Management in VANET, *Proceeding of the 2nd International Conference on Future Computer and Communication (ICFCC 2010), Wuhan, China, 21, May 2010.*