International Journal of Engineering Research-Online
A Peer Reviewed International Journal
Email:editorijoer@gmail.com http://www.ijoer.in

Vol.4., Issue.2., 2016
(Mar-Apr)

REVIEW ARTICLE

ISSN: 2321-7758

VANET: OVERVIEW, SECURITY ISSUES AND CHALLENGES

BAPPADITYA JANA[1], JAYANTA PORAY[2]

[1,2]Department of Computer Science & Engineering
Techno India University
EM-4, Sector-V, Salt Lake, Kolkata-700091
West Bengal, India

ABSTRACT

In the current era of rapid advancement of Information Technology and Communication, VANET (Vehicular Ad-hoc Networks) has received immense attention from academia, industry and government in all over the world. In fact, due to the change of life style the number of Vehicles on roads increases day by day. Accidental phenomenon caused by reckless driving has yet not been stopped, in spite of several preventive measures. Again, the scope for enhancement of road infrastructure is mostly saturated. Safety distance between two adjacency vehicles and maintaining the reasonable speed of vehicles are hardly respected. Drivers are often driving their cars with lack of attention. As per the current statistical report, ten among thousand of people die and hundred among thousand of people get injured in traffic accidents all over the world in each year. So the life risk situation is very high in VANET. In the case of traditional networks or conventional mobile networks, security and privacy failures usually bring financial losses, where as in VANET, both security and privacy failures could be much more serious life risk factors. So VANET has emerged as an exciting research and application area for network security. In this paper we have tried to discuss about the overview of VANET infrastructure, some applications and some serious technical and security issues to implement an ideal VANET. We have also mentioned some major attacks on VANET. Here we aim to have detail insight into the overall matter, which will help protocol designers and applications engineers to improve the services provided in VANET and assist drivers to incorporate more on road security and comfort.

Keywords: VANET, MANET, Network Security, Intelligent Transport System.

I. INTRODUCTION

VANET is a promising area for future ITS (Intelligent Transport System). Vehicular Ad-hoc Networks (VANET) represents a challenging class of MANET (Mobile Ad Hoc Networks) that enables vehicles to intelligently communicate with each other and with roadside infrastructure[2]. VANE is a subset of MANET[4]. There are some limitation of MANET such as packet delivery delay, involving packets being dropped, wasting bandwidth, mobility and security. To overcome these limitations many routing algorithm have been proposed in MANET. But these techniques can not be adopted for VANET because of some special characteristics (Such as restricted mobility pattern of VANET). In VANET vehicles form a self organised network without the help of a parmanent infrastructure Network. Driving means constantly change of location. It means a constant demand for information on the current location and specifically for data on surrounding

traffic routes and much more. The use of Radio Communications for vehicle to Vehicle and Vehicle to roadside in order to increase traffic safety, to increase traffic efficiency and to increase environmental friendliness. VANET have various potential applications. The main thrusting area of researchers on VANET's to implement traffic safety application[27]. Major number of traffic accidents caused from lack of co operation between drivers. If actual traffic information can be send to the drivers through VANETs,then they can overcome all possibilities of conflicts and most life endangering accidents.

II. VANETS ARCHITECTURES OVERVIEW

VANET (Vehicular ad-hoc networks) is a wireless network that is formed between vehicles on an as need basis [11]. Vehicles must be equipped with wireless transceivers and computerized control modules in order to participate in VANET and acts as network nodes. VANET is also called as inter-vehicle communications (IVC) or vehicle to Vehicle (V2V) communications [12]. VANET turns each participating vehicles into a wireless router or nodes to connect to form a wide network, since each individual node's wireless network range may be limited to few meters, so by hopping through several nodes it provides end to end communication across longer distances[11].

Basic Components of VANET:

- **Vehicle To Infrastructure (V2I)**
- **Vehicle To Vehicle (V2V)**
- **Road Side Unit (RSU)**
- **On Board Unit (OBU)**

Unique characteristics of vanet:-

A.High Mobility of Node: Nodes(Vehicle) in a VANET moves with high mobility and some time vehicles cross each other and they exchange packets in a milliseconds. Mobility of nodes is depend on road structure and traffic rules. Network Topology also changes with movement of nodes.

B.Unbound Network Size

VANET is technically an ITS(Intelligent Transport System) with large no of nodes. Vehicles and some potential roadside Units(RSU).Vehicles in VANET could be in one city,several cities or even a country.VANET is the independent of number of nodes.

C.Time Sensitive Data Exchange

Security issues of VANET need message delivery without any delay..Becayse any type of accident may takes place within a milliseconds.

D.Potential Support from Infrastructure

Road units basically road infrastructure gives an extra potential support to VANET .

E.Unlimited Battery Power and Storage

Nodes in Vanets do not suffer power and storage limitation as in sensor networks.

F. No Confidentiality

In case of safty issue,the information contained in the alert message is available and applicable for all vehicles in VANET as the main aim to avoid accidents. So there is no need of confidentiality in the message

III.APPLICATION OF VANET

We are arranging VANET application in the following classes:

A.Safety Oriented:

Safety applications will monitor the surrounding road approaching vehicals,surface and curve of the road.

B.Commercial applications

It will provide the driver with the entertainment and services as web access,streaming audio and video.

C. Convenience application

These are mainly of traffic management type such as automatic parkong,automatic toll collection etc.

D.Productive applications

These are the real application derived from above three types application.This type of application helps to minimize fuel,time and other cost related with Vanets.

A. Safety Oriented:

1.Traffic signal

Communication from traffic light can be created with technologies of VANET, Co-operative Message Transfer: safety applications would be slow/stop vehicle advisor (SVA) in which a slow or motionless vehicle will broadcast alert message to its neighborhood congested road notification(CRN) detects and notifies about road congestions which can be used for rout and journey planning. The toll

collection [19] is yet another application for vehicle tolls collection at the tollbooths without stopping the vehicles.

2.Real Time Traffic: The real time traffic data can be stored at the RSU by geocasting and can be available to the vehicles whenever and wherever needed.

3.Post Crash Notification: After accident A vehicle would broadcast the warning messages about its position to trailing vehicle so that it can take decision with time in hand.

4.Vision Enhancement: In vision enhancement, drivers are given a clear view of vehicles and obstacles in heavy fog conditions and can learn about the existance of vehicles hidden by obstacles,buildings and other vehicles.

5.Weather Conditions: Either vehicle sensors (Wipers movement,grip control, outside thermometer etc) if not available or reliable,weather information can be updated /requested by an application via DSRC In post crash notification , a vehicle involved in an accident would broadcast warning message about its position to trailing vehicles so that it can take decision with time in hand as well as pass information in the high way patrol for support parking Availability notification (PAN) helps to find the availability of space in parking lot in a certain geographiocal area as per the weather conditions.

For the convenience of the vehicle high way and urban area maps are avaible which avoid the traffic jam and accident conditions and also provide shortest path in critical situation which saves the time.

6.Driver Assistance: Vehicular networks can also be used to support driving military exercises by providing drivers with information that they might have missed or might not yet be able to see.By[**20]** having vehicles exhibiting abnormal driving patterns,such as a dramatic change of direction,send messages to inform cars in their locality,drivers can be warned earlier of potential hazards and therefore get more time to react and avoid accidents.

B.Commercial Application:

1.Searching Road side Locations and Vehicles Direction

Passenger can download digital road map through VANET.For unknown passenger help to find the shopping center,hotels ,gas stations etc in the nearby area along the road GPS,sensors and database station are capable of calculating information.

2.Real Time Video Relay: Drivers can view real time video relay.

3.Value Added Advertisement: This service is given by service providers who want to attract customers to their stores like petrol pumps, highway Café area, hotels within communication range. This facilities can be available in absence of internet also.

C.Convenience application

1.Automatic Parking: Automatic parking is an application through which a vehicle can park itself without the need for driver intervention.

In order to be able to perform an automatic parking,a vehicle needs accurate distance estimators and/or a localization system with submeter precision.

2.Automatic Toll collection: A Toll collection point can be able to read the OBU of the vehicle through GPS[17] and the on board odometer or techograph as back up to determine how far the vehicle have travelled by reference to a digital map and GSM to authorize

the payment of the toll via wireless link.

3.Enhancement of Road Infrastructure: Using Vanet we can modify actual road diversion.

D.Productive applications:These are basically gives mimimization of cost and time.

Fuel and Time saving: In Toll booths , cars have to wait and the same time they do not stop their engine. So in case of automatic toll collection drivers can save both fuel as well as time.

IV. CHALLENGING ISSUES IN VANET

Vanet involves number of challenges in terms of Quality of service (QoS) and its performance.Due to the small failure of both may cause serious traffic accidents with loss of lives. QoS depends on numerous parameters such as bandwith,packet delivery raio,data latency ,delay variance etc. The main objectives of VANET is to provide safety to Vehicles.Some challenges of VANET are security,reliability and confidentiality in data

transmission that also affects the QoS. A final challenge comes from the time constraints of the envisioned safety and driver assistance applications.In case of emergency braking,milliseconds of delay may cause a serious traffic accident.Hence emergency messages must be generated by the sender and verified by receiver as soon as possible. Unless proper measures are taken, a number of attacks could easily be conducted, namely message content modification, identity theft, false information generation and propagation etc .

A. Technical Challenges

The technical challenges deals with the technical obstacles which should be resolved before the deployment of VANET.

1.Network Topology Management: Due to high mobility node, the network topology also be changeable. So it is impossible to use static tree base network topology. The unbounded network size is the another issues. The size of VANET.s involves in a metropolitan areas with millions of Vehicles is another challenge. Again Number of nodes in metropolitan city Vs urban area; day time Vs night are variable which is the one of the main cause of network congestion.

2. Environmental Impact In VANET: electromagnetic waves is used for communication which can affect environment especially living beings.

3. MAC Design: VANET generally use the shared medium to communicate hence the MAC design is the key issue. Many approaches have been given like TDMA, SDMA, and CSMA etc. IEEE 802.11 adopted the CSMA based Mac for VANET.

4. Security: Security is provided by different ways like authentication and encryption.

B. Socio-Economical and Political challenges: :

Due to the illetaracy it is very difficult to convince to some class of peipole to maintain besic traffic rules in VANET. The same problem may arrise in case of economically extreme high class of people,they can reject primary traffic rules.Conversely they appreciates the warningmessage of police trap. Sometimes transportation system are governed by a multitude of authorities with different interests, which complicates the rules.

V. SECURITY ISSUES IN VANET

VANET packets contains life critical information hence it is necessary to make sure that these packets are not injected or modified by the attacker. These security problem are not same with general communication network.

A. Security Challenges in VANET

To overcome security challenges in VANET ,we have to deeply concentrate in the design of VANET architecture, security protocols, cryptographic algorithm etc. The following list presents some security challenges [2]:

1.Real time Constraint*:* VANET is time critical where safety related message should be delivered with 100ms transmission delay. So to achieve real time constraint, fast cryptographic algorithm should be used. Message and entity authentication must be done in proper time.

2.Data Consistency Liability: In VANET even authenticate node can perform malicious activities that can cause accidents or disturb the network. Hence a mechanism should be designed to avoid this inconsistency

3.. **Low tolerance for error**: Some protocols are designed on the basis of probability. VANET uses life critical information on which action is performed in very short time. A small error in probabilistic algorithm may cause harm.

4.KeyDistribution: All the security mechanisms implemented in VANET dependent on keys. Each message is encrypted and need to decrypt at receiver end either with same key or different key. Also different manufacturer can install keys in different ways and in public key infrastructure trust on CA become major issue. Therefore distribution of keys among vehicles is a major challenge in designing a security protocols.

5. High Mobility: The computational capability and energy supply in VANET is same as the wired network node but the high mobility of VANET nodes requires the less execution time of security protocols for same throughput that wired network produces. Hence the design of security protocols must use the approaches to reduce the execution time. Two approaches can be implementing to meet this requirement.

a) ***Low complexity security algorithms****:* Current security protocols such as SSL/TLS, DTLS, WTLS, generally uses RSA based public key cryptography. RSA algorithm uses the integer factorisation on large prime no. which is NP-Hard. Hence decryption of the message that used RSA algorithm becomes very complex and time consuming. Hence there is need to implement alternate cryptographic algorithm like Elliptic curve cryptosystems and lattice based cryptosystems. For bulk data encryption AES can be used.

b) ***Transport protocol choice****:* To secure transaction over IP, DTLS should be preferred over TLS as DTLS operates over connectionless transport layer. IPSec which secures IP traffic should be avoided as it requires too many messages to set up. However IPSec and TLS can be used when vehicles are not in motion.

B. Security requirements in VANET

Some basics requirement is needed to design a good VANET infrastructure. A security system in VANET should satisfy the following requirements [5]:

1.Authentication: The Authentication service is concerned with assuring that the communication is authentic in its entities. Vehicle should react to events only with disseminating messages generated by legal senders. Threrefore we need to authenticate the senders of these messages.

2.Availability: Availability requires that the information must be available to the legitimate users. DoS Attacks can bring down the network and hence information cannot be shared.

3.Non-Repudiation: Non-repudiation means a node cannot deny that he/she does not transmit the message. It may be crucial to determine the correct sequence in crash reconstruction.

4.Privacy: The privacy of a node against the unauthorised node should be guaranteed. This is required to eliminate the massage delay attacks.

5.Data Verification*:* A regular verification of data is required to eliminate the false messaging.

6.Integrity **:** The integrity service deals with the stability of a stream of messages. It assures that messages are received as sent,without modification,insertion reordering or replays.

7.Confidentiality**:** This service provides the confidentiality to the communication content. It guarantees the privacy of drivers against unauthorized obsevers.

8.Scalability**:** The term scalability means that the number of users and/or the traffic volume can be increased with reasonably small performance degradation or even network outage and without changing the system components and protocols.

9.Reliability Due to the breif communication time,it is difficult to assure the reliable message reception and acknowledgement between communication vehicles on opposite directions. In vehicular ad hoc networks a majority of the message that announce the state of vehicle to it neighbours. so in case of broadcast message it needs more reliability.

C. Attackers on Vehicular Network

To secure the VANET, first we have to discover who are the attacker, their nature, and capacity to damage the system. On the basis of capacity these attackers may be three types [5].

1.Insider and Outsider: Insiders are the authenticated members of network whereas Outsiders are the intruders and hence limited capacity to attack.

2.Malicious and Rational: Malicious attackers have not any personal benefit to attack; they just harm the functionality of the network. Rational attackers have the personal profit hence they are predictable.

3.Active and Passive:: Active attackers generate signals or packet whereas passive attackers only sense the network.

D. Attacks in the VANET

To get better protection from attackers we must have the knowledge about the attacks in VANET against security requirements. Attacks on different security requirement are given below [7]:

1.Impersonate**:** In impersonate attack attacker assumes the identity and privileges of an authorised node, either to make use of network resources that may not be available to it under normal circumstances, or to disrupt the normal functioning of the network. This type of attack is performed by active attackers. They may be insider or outsiders. This attack is multilayer attack means attacker can exploit either network layer, application layer or

transport layer vulnerability. This attack can be performed in two ways:

a) False attribute possession*:* In this scheme an attacker steals some property of legitimate user and later with the use of attribute claims that it is who (legitimate user) that sent this message. By using this type attack a normal vehicle can claim that he/she is a police or fire protector to free the traffic.

***b)Sybil*:** In this type of attack, an attacker use different identities at the same time.

2.Session hijacking: Most authentication process is done at the start of the session. Hence it is easy to hijack the session after connection establishment. In this attack attackers take control of session between nodes.

3.Identity revealing: Generally a driver is itself owner of the vehicles hence getting owner's identity can put the privacy at risk.

4.Location Tracking: The location of a given moment or the path followed along a period of time can be used to trace the vehicle and get information of driver.

5.Repudiation: The main threat in repudiation is denial or attempt to denial by a node involved in communication. This is different from the impersonate attack. In this attack two or more entity has common identity hence it is easy to get indistinguishable and hence they can be repudiated.

6.Eavesdropping is a most common attack on confidentiality. This attack is belongs to network layer attack and passive in nature. The main goal of this attack is to get access of confidential data.

7.Denial of Service: DoS attacks are most prominent attack in this category. In this attack attacker prevents the legitimate user to use the service from the victim node. DoS attacks can be carried out in many ways [8].

a)Jamming: In this technique the attacker senses the physical channel and gets the information about the frequency at which the receiver receives the signal. Then he transmits the signal on the channel so that channel is jam.

b)SYN Flooding*:* In this mechanism large no of SYN request is sent to the victim node, spoofing the sender address. The victim node send back the SYN-ACK to the spoofed address but victim node does not get any ACK packet in return. This result too half opens connection to handle by a victim node's buffer. As a consequence the legitimate request is discarded.

c)Distributed DoS attack*:* This is another form Dos attack. In this attack, multiple attackers attack the victim node and prevents legitimate user from accessing the service.

8.Routing attack: Routing attacks re the attacks which exploits the vulnerability of network layer routing protocols. In this type of attack the attacker either drops the packet or disturbs the routing process of the network. Following are the most common routing attacks in the VANET:

a)Black Hole attack: In this type of attack, the attacker firstly attracts the nodes to transmit the packet through itself. It can be done by continuous sending the malicious route reply with fresh route and low hop count. After attracting the node, when the packet is forwarded through this node, it silently drops the packet.

b)Worm Hole attack: In this attack, an adversary receives packets at one point in the network, tunnels them to another point in the network, and then replays them into the network from that point . This tunnel between two adversaries are called wormhole. It can be established through a single long-range wireless link or a wired link between the two adversaries. Hence it is simple for the adversary to make the tunneled packet arrive sooner than other packets transmitted over a normal multi-hop route.

c)Gray Hole attack: This is the extension of black hole attack. In this type of attack the malicious node behaves like the black node attack but it drops the packet selectively. This selection can be of two type:

I. A malicious node can drop the packet of UDP whereas the TCP packet will be forwarded.
II. The malicious node can drop the packet on the basis of probabilistic distribution.

That is why designing secure and functional VANET is a challenging Problem**.**

VI. CONCLUSION

Actually it is not a surprise that VANET,s is almost suitable for delivering content in vehicular application but there are also a lot of issues which has to be solved before practical application implementation of VANETs network. Security and privacy are the two critical issues to implement a ideal VANETs.. In this paper, we first have given a description of VANET architecture, followed by the characteristics described in Section II. Section III describes various applications of VANET.In Section IV we have analyzed various challenging issues to implement an ideal VANET. At last , section-v have shown a group of security issues at present and in future in ongoing research on VANET. Although the works on VANET are numerous, but there are still issues which may be untouched. So. We hope, at least, the study in this paper would contribute in new research directions.

References

[1]. M.Raya and J.P . Hubaux, 'The security of Vehicular Ad Hoc Networks". In ACM SASN,pp 11-21,2005

[2]. P.Papadimitratos, L Buttyan , T Holczer , E Schoch, J Freudiger, M . Raya, Z Ma, F Kargi, A kung and J-P Hubaux," Secure communication systems. Design and Architecture," IEEE communications Magazine, Vol.46, no 11,pp 100-109,2008

[3]. B. Lynn, "On the Implementation of Pairing-Based Cryptosystems," Ph.D. dissertation, Stanford University, 2007

[4]. S. K. V. L. Reddy, S. Ruj, and A. Nayak, "Data authentication scheme for unattended wireless sensor networks against a mobile adversary," in 2013 IEEE Wireless Communications and Networking Conference (WCNC), Shanghai, Shanghai, China, April 7-10, 2013. IEEE, 2013, pp. 18361841.[Online].Available:http://dx.doi.org/10.1109/WCNC.2013.6554843

[5]. Maxim Raya e al.,"The Security of Vehicular Ad Hoc Networks", SASN'05, Nov 7 2005,Alexandria, Verginia, USA, pp. 11-21

[6]. Hannes Hartenstein et al., "A tutorial survey on vehicular Ad Hoc Networks" , IEEE Communication Magazine, June 2008, pp. 164-171

[7]. Jose Maria de Fuentes, Ana Isabel Gonzalez-Tablas, and Arturo Ribagorda, "Overview of Security issues in Vehicular Ad Hoc Networks", Handbook of Research on Mobility and Computing, 2010.

[8]. Murthy, C. S. R.,Manoj, B. S.: Ad Hoc Wireless Networks: Architectures and Protocols. PEARSON,ISBN 81-317-0688-5, (2011)

[9]. Schmidt RK, Leinmuller T, Schoch E, Held A, Schafer G (2008) Vehicle behavior analysis to enhance security in vanets. In:Workshop on vehicle to vehicle communications 24. Zhang J, Chen C, Cohen R (2010) A scalable and effective trust-based framework for vehicular ad-hoc networks. JoWUA 1(4):3–15

[10]. "A Comparative study of MANET and VANETEnvironment."[Online].Available:http://www.scribd.com/JournalofComputing/d/34832829-A-Comparative-study-of-MANET-andVANETEnvironment#download. [Accessed: 18-Jun-2012].

[11]. J. Bernsen, "A_Reliability-Based Routing Protocol for Vehicular Ad- Hoc Networks," Master's Theses, Jan. 2011.

[12]. F. Li and Y. Wang, "Routing in vehicular ad hoc networks: A survey," Vehicular Technology Magazine, IEEE, vol. 2, no. 2, pp. 12 –22, Jun. 2007.

[13]. Y. Toor, P. Muhlethaler, and A. Laouiti, "Vehicle Ad Hoc networks: applications and related technical issues," Communications Surveys Tutorials, IEEE, vol. 10, no. 3, pp. 74 –88, quarter 2008.

[14]. Y. Toor, P. Muhlethaler, and A. Laouiti, "Vehicle Ad Hoc networks: applications and related technical issues," Communications Surveys Tutorials, IEEE, vol. 10, no. 3, pp. 74 –88, quarter 2008.

[15]. "User requirements model for VANET applications."[Online].Available:http://mimos.academia.edu/JamalullailAbManan/Papers/963337/User_requirements_model_for_VANET_applications. [Accessed: 20-Jun-2012].

[16]. Hongmei Deng, Wei Li, and D. P. Agrawal, "Routing Security in Wireless Ad Hoc Networks", IEEE Communications Magazine, Vol.40, No.10, pp.70-75,October 2002.

[17]. R. B. Thompson, "Global Positioning System (GPS): The Mathematics of Satellite Navigation," MathCAD library, http://www.mathsoft.com/appsindex.html. 1998.

[18]. Kejie Lu, Shengli Fu, and Yi Qian, "On the Design of Future Wireless Ad Hoc Networks", Proceedings of IEEE GLOBECOM'2007, November 2007.

[19]. T. ElBatt, S. Goel, G. Holland, H. Krishnan, J. Parikh, "Cooperative Collision Warning Using Dedicated Short Range Wireless Communications", 3rd ACM International Workshop on VANETs, Los Angeles, California, USA, 2006.

[20]. F. Dötzer, F. Kohlmayer, T. Kosch, M. Strassberger "Secure Communication for Intersection Assistance", in Proc of the 2nd International Workshop on Intelligent Transportation, Hamburg, Germany, March 15-16, 2005.

[21]. Qian, Yi, Nader Moayeri. "DESIGN SECURE AND APPLICATION-ORIENTED VANET", National Institute of Standards and Technology.Apr2009:http://w3.antd.nist.gov/pubs/Yi-Paper7.pdf.

[22]. H. Wu, R. Fujimoto, R. Guensler, M. Hunter, "MDDV: A Mobility-Centric Data Dissemination Algorithm for Vehicular Networks," in 1st ACM workshop on vehicular ad hoc networks, Oct. 2004, pp. 47 – 56.

[23]. U.S.DepartmentofTransportation,Intelligent Transportation Systems(ITS)Home,http://www.its.dot.gov/index.htm

[24]. Zeyun N. , Wenbing Y. , Qiang N., Yonghua S., "Study on QoS Support in 802.1le-based Multi-hop Vehicular Wireless Ad Hoc Networks", in Proc. IEEE International Conference on Networking, Sensing and Control, London, April 2007, pp-705-71

[25]. H. Hartenstein, B. Bochow, A. Ebner, M. Lott, M. Radimirsch, D. Vollmer, "Position-aware ad hoc wireless networks for inter-vehicle communications: the Fleetnet project," in Proceedings of the 2nd ACM international symposium on Mobile ad hoc networking & computing, Oct. 2001, pp. 259 - 262.

[26]. International Journal of Network Security & Its Applications (IJNSA), Vol.5, September 2013

[27]. R. D. Pietro, S. Guarino, N. V. Verde, and J. Domingo-Ferrer,"Security in wireless ad-hoc networks - A survey," Computer Communications, vol. 51,pp.120,2014.[Online].Available:http://dx.doi.org/10.1016/j.comcom.2014.06.003

[28]. Zhang J (2011) A survey on trust management for VANETs. In: 25th IEEE international conference on advanced information networking and applications, pp 105–112

[29]. R. D. Pietro, S. Guarino, N. V. Verde, and J. Domingo-Ferrer, "Security in wireless ad-hoc networks - A survey," Computer Communications, vol. 51, pp. 1–20, 2014. [Online].http://dx.doi.org/10.1016/j.comcom.2014.06.003

[30]. R. D. Pietro, L. V. Mancini, C. Soriente, A. Spognardi, and G. Tsudik,"Catch me (if you can): Data survival in unattended sensor networks, "in Sixth Annual IEEE International Conference on Pervasive Computing and Communications (PerCom2008),17-21 March 2008, Hong Kong.IEEE,ComputerSociety,2008,pp.185194.[Online].Available:http://doi.ieeecomputersociety.org/10.1109/PERCOM.2008.31

[31]. A.Prado, S. Ruj, A. Nayak IEEE - Enhanced Privacy and Reliability for Secure Geocasting in VANET, ICC 2013 - Ad-hoc and Sensor Networking Symposium

[32]. S. K. V. L. Reddy, S. Ruj, and A. Nayak, "Distributed data survivability schemes in mobile unattended wireless sensor networks," in *2012 IEEE Global Communications Conference, GLOBECOM 2012, Anaheim, CA, USA, December 3-7, 2012*. IEEE, 2012, pp. 979–984. [Online]. Available:http://dx.doi.org/10.1109/GLOCOM.2012.6503240