Using Computing Methods to Secure Vehicular Ad hoc Network (VANET): A Survey

Irshad Ahmed Sumra

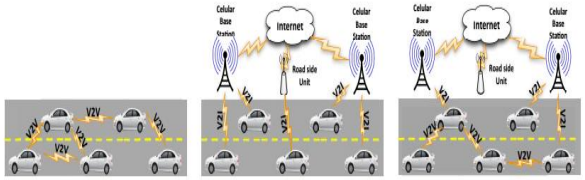
***Abstract*—VANET is next generation vehicular network and its applications will be play key to safe human life while journey on highway. Security is one of the key prominent factors for implement VANET in real environment. Different researchers already provides different solutions to make it secure from attacker and attacks in network. In this survey paper, discuss in detail the various computing methods and illustrate the relationship with vehicular network. Using these computing methods to secure the vehicular network from attackers and attacks. Trusted computing and Cloud computing are some of the types of computing methods which are already discussed in VANET. But still some computing method need to discuss the relationship with VANET and its security like Quantum computing and Pervasive computing.**

***Index Terms*—Application, security, computing methods, trusted computing, cloud computing, pervasive computing.**

I. Introduction

Recent year's transportation issues and traffic activities are play vital role in daily life upbringing. So, increase the level of improvement is most important to the growing the better vehicle system. One side day by day Transportation system is damage in the cause of huge amount of traffic and the other side significantly increases the level of accident. Novel technologies have been investigate connecting to the Vehicular Ad Hoc Network (VANET) due to enhancement in vehicular traffic/overcrowding around us [1]. VANET is a basically development system that increase the traffic safety and reduce the traffic accidents. VANET is a wireless technology that moves the car through the nodes and transfers the messages one node to another node. Node are communicating single hop multi hop and also provide the huge range of network to capture the signals and send the messages. Defiantly, VANET technology enhances the security and traffic transportation [2]. Vehicular communication is involved of the nearby vehicles and the appropriate design of VANET to provide the better safety driving. According to the Nazish [3] therefore VANET provide the complete computing environment facilitate various services through a assortment of applications. Fig. 1 show the architecture of VANET.

VANET security requirements and in section III briefly discuss the basic security challenges in vehicular environment. The sections IV describes the different types of computing methods and discuss in detail the relationship of VANET security with these computing methods. Section V concludes the paper.



(a) Vehicle-to-Vehicle Ad Hoc Network (b) Vehicle-to-Infrastructure Network (c) Hybrid Architecture

Fig. 1. VANET architecture [3].

II. Security Requirements

Security and privacy pay an important role to make the VANET superstitions, popular and unique all the transportation system. For this purpose identify the some security requirement to fulfill the privacy needs and provide secure wireless communication between the two vehicles. Data transformation in secure manner and protect the attacker. In the case of accident provide the awareness to the drivers and helps to take any action such a ridicules situation. Security sight VANET determine be additional challenges [2]. Actuality, every communication model has a special set of security requirements.

- Identification
- Authentication
- Element authentication
- Privacy conservation
- Non- repudiation
- Confidentiality
- Availability
- Trust

This table contains the verification of requirement different communication system. Illustrate the communication system authenticate the requirements according to the security condition and fulfill the vehicle needs depending the situation.

Identification: Each entity enclose unique value and different to the other entity. Vehicular Identification contains number or VIN. Registration number demonstrates the identity certificate for each vehicle.

Authentication: Prove the unique identity is called authentication. Authentication is an approval stage and verifies that the communication of vehicles is secure and attacker interrupts in the conversation.

Manuscript received February 12, 2018; revised April 20, 2018.

Irshad Ahmed Sumra is with Computer Science Department, University of South Asia, 47-Tufail Road, Lahore, Pakistan (e-mail: irshad.ahmed@usa.edu.pk).

doi: 10.18178/jacn.2018.6.1.256

Element authentication: The only need is to show that both participating entities have the required attributes to become group members – this is the attribute authentication requirement [3].

Privacy conservation: Privacy is significant for vehicles. User privacy is more important in VANET because of fulfill the purpose of secure communication. In the vehicular perspective, privacy is accomplish two associated objective are contented untraceability and unlink ability.

Untraceability*:* The *v*ehicle proceeding not be traced (i.e. different achievement of the identical vehicle should not be interconnected).

Unlinkability*:* It should be unfeasible for an illegal entity to associate vehicle uniqueness with that of its driver/owner.

Non-repudiation: One more condition for VANETs is non-repudiation, which means that users ought to not be capable to refuse transfer a message so that they preserve is follow and castigate in container of a false message.

Confidentiality: In group communication massage will only read authorize party So that secure communication built in both parties. Only group members read the information.

Availability: Each node is alert and active to send the information to the other node because these connectivity very important to the road safety this is vital a requirement to the security.

Trust: Data integrity and correctness must be ensured in trust procedures. Straightforwardly data is important should not be modify so that trust is an important requirement for VANET communication.

TABLE I: SECURITY REQUIREMENTS IN VANET [3]

VANET setting / Sec. Requirement	V2V warning propagation	V2V group communication	V2V beaconing	I2V warning	V2I warning
Entity identification	✓ (all vehicles)	x	✓ (sender)	✓ (sender)	✓ (sender&receiver)
Entity authentication	✓ (sender)	x	✓ (sender)	✓ (sender)	✓ (sender&receiver)
Attribute authentication	x	✓ (sender&receiver)	x	x	x
Privacy preservation	✓	✓	✓	x	✓
Non-repudiation	✓ (sender)	x	✓ (sender)	✓ (sender&receiver)	✓ (sender&receiver)
Confidentiality	x	✓	x	x	x
Availability	✓	✓	✓	✓	✓
Data trust	✓	✓	✓	✓	✓

III. SECURITY CHALLENGES IN VANET

Here is providing the detail description of security challenges in VANET.

- Real Time Constraints: VANET achieve the real time constraints so, required the specific timing to deliver the massages. Achieve this goal use very fast cryptographic algorithm.
- Data consistency Liability: Data consistency is important in VANET and avoids the unnecessary information because authenticate node execute the malicious.
- Key Distribution: VANET use the key to send and receive the messages encrypts the message and after procedure complete decrypt the message that's why key distribution is an important procedure and perform the major challenge.
- High mobility: High mobility is required in VANET nodes are connected each other's and transfer the signals to communicate the other vehicle so very fast mobility level is required. VANET required less execution time.
- Non- repudiation: In this procedure node cannot refuse but does not send the messages and signals. It's going to be crucial to work out the proper sequence in crash re-establishment [2].
- Data verification and privacy: To preserve the integrity, regular bases check the verification and privacy is very essential characteristic in VANET.

IV. COMPUTING METHODS – VANET SECURITY

Security is still open challenges in vehicular network due to dynamic topology and dynamic behavior of attacker in network. Many security solutions already provided for VANET and in this section, we will review the previous work and also discuss the some new computing methods to secure the vehicular network. The Fig. 2 shows the different types of computing methods and in this section provides detail discussion with respect to VANET security.

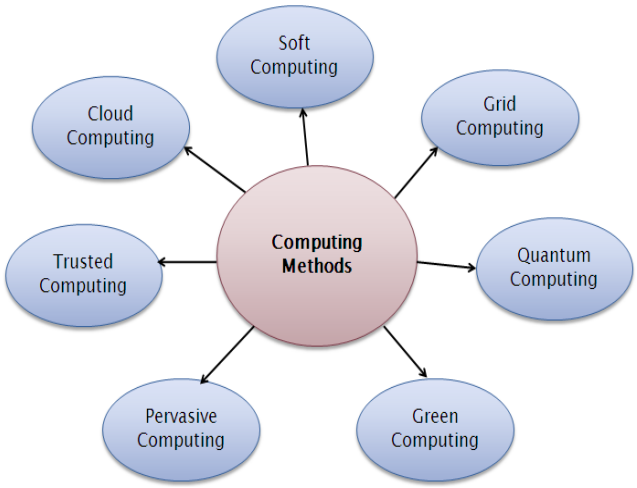


Fig. 2. Different types of computing methods.

A. Cloud Computing and VANET

Accomplishment of cloud computing application obtain the advanced prerequisites and providing proper resources, services acquire and programs Therefore cloud computing applications intend a capable results to resolve such problems. Cloud computing is a latest computational modal that propose pioneering production replica for association to implement IT lacking blunt savings however, achieve the potential gains such that cloud computing is one of the hottest area in the field of information Technology and also have technological, financial and user friendly characteristic. Some key point present the cloud computing fault tolerance loose coupling, service oriented, pay per use provide the services on demand, cost effective etc. Cloud computing facilitate the developing technology for industry and

academic purposes. VANET is the hottest topic now a day that use the communication nodes to communicate one vehicles to another' s use the wireless networks sensors to sense the data VANET is delivered form to MANET (mobile ad-hoc network) but VANET behavior is not some of the MANET[2]. Some VANET issues resolve the cloud Security and Cost also these are two important challenges of VANET.

VANET propose early detections system commencing hazard (risk warning) for drivers so, security is major and important component for VANET. Three methods were proposed to protect vehicular system against intentional re-get of the region of vehicle by hackers which are: plausibility checks [3], logic reception beacons [4] and tamper proof GPS [5]. In accumulation, are two kinds of method to suggest data-centric secure and authenticate in the vehicular networks responsive and active security. Three variety of replica to legitimize and to combine the position of information in a Vehicular Cloud (VC) are: An active location integrity model, passive location truthfulness and finally, position integrity model [2]. In Tang *et al.* [6] the authors recommended a way to observe if the accurate position of a collection of associated vehicles by using the locations of hug vehicles which known as "Secure Relative Location Determination in Vehicular Network" (SRLD) [7] although a localization method which relies on insolvency malevolent data is referred in given study [7]. Yan *et al.* in [8] established by state a location of the justification technique to make confident of vehicles locations. To revolve the location into a key (geo-lock), an encryption algorithm is desirable; consequently it's achievable to develop the position error staying power in transportation networks.

B. Grid Computing and VANET

Vehicular ad-hoc network with grid computing energetically uses significant data to execute computations for solve traffic associated issues and the motive is to develop intelligent vehicles, in which vehicle prepared with wireless networking and computers can cooperate, solves the transportation problems of vehicles. V Grid, vehicles play the major responsibility mobile sensors (collecting data) and mobile routers (transmit data), also connected cooperatively to appearance of a global grid computer. High density car use the high density potential node to perform the distributed computations. VGrid computing network ability can facilitate safety applications for vehicle driver and self-sustaining to disaster situation. Joey *et al.* [2] introduce proposed framework V Grid. This framework proposes the unique functional elements such that unchanging road side sensor, vehicle sensor, central management canter and variable message signs and also per pose two line merging scenario into one.

C. Green Computing and VANET

Vehicular ad-hoc network is the category of MANET. Vehicular network move the vehicle boundaries of wireless nodes by using sensor. Sensors sense the data and communicate one vehicle to the other vehicle. VANET basically depend on a smart cars and base stations these base stations allocate the information through the wireless nodes. Rashid *et al*. [4] purpose green vehicle communication Green vehicle transportations necessities are accessible to illustrate the consequence of using vehicular technology and test using NS-2 to calculate the average delay time per trip and average throughput for three different situation are existing and spotlights some major requirement for green vehicle communication. In this figure the ORDC monitors and controls the operational rescue that involves multiple teams [4]. The Fig. 3 shows the operation model in green computing in vehicular environment.

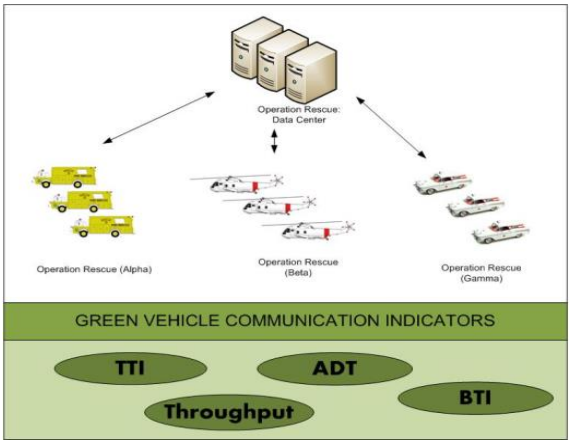


Fig. 3. Operation rescue modal [4].

Suganyal *et al.* [5] demonstrate a model of Authentication Structure with Restricted Privacy-Preservation and Non-Repudiation automobile way to compact with strengthens green automobile communication for urban procedures defend. Author illustrates the green computing technology on VANET using ACPN method. ACPN is the privacy conservation that contains authentication and validity process. Catalogue some VANET challenges to show the affect future vehicle communication and much better results as compare to recent vehicles such that design of the vehicle , hardware capacity, create the new VANET technologies in markets, new wireless broadcast sachem implement , major issue is security so, so introduce the privacy models and use the beneficial technologies in VANET.

D. Soft Computing and VANET

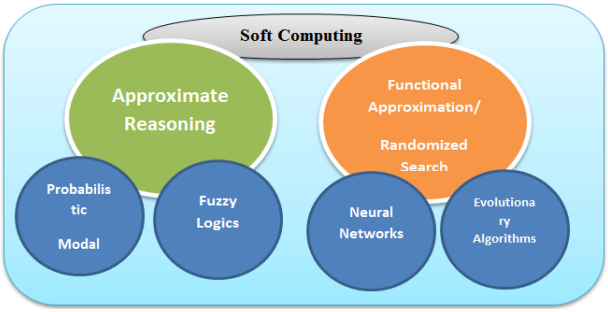


Fig. 4. Soft computing [4].

Collection of the computational techniques of the computer science is the part of the soft computing also artificial intelligent, machine learning and very complex phenomena also refer to the soft computing very low cost and computational methods. Previous computational modal investigate only relatively simple system and modern complex computing include biological method, medicine, management science etc. both systems (simplicity and complexity) are relative and conventional throughput [6].Soft computing contains residents like fuzzy sets, neural networks,

and genetic algorithms [7]. The basically soft computing as instigate human nature and intelligent and Fig. 4 describes the soft computing. Soft computing is not a homogenous body is to adventure the acceptance for fuzziness and improbability to achieve the controllability.

E. Trusted Computing and VANET

In the recent years trust play vital role in the security and challenge activities and grown popularity the main component of trusted computing is the trusted computing group (TCG) the TCG improve the security in computer networks through TPM [9]. According to the A.L thorp Trust is the key security module of any system .Trusted computing modules establish the trust and increase the security levels and protect the hackers. Irshad *et al.* [8] proposed trusted modal for vehicular ad- ad hoc networking environment. The proposed modal contains two different models. First module based on attacker and the attacks as well as second module based on trust and trusted computing technologies. Fig. 5 describes the trust and trusted model in VANET.

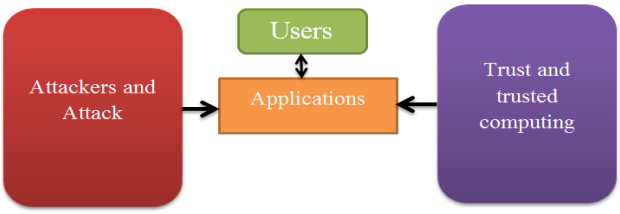


Fig. 5. VANET trust and trusted modal [10].

Irshad *et al* [10] introduced the proposed modal for the trusted computing Vehicular ad-hoc network. In this paper a protocol is proposed which is constructed on a property based attestation (PBA) similarly recognized as Vehicular Property established attestation Protocol (VPP).

F. Quantum Computing and VANET

Quantum computing is the combination of the concept quantum physics and computer science these computers are more powerful and fundamental. The ability of quantum computing is to very efficiently process the algorithms which are more difficult to processing [11]. Quantum computing performance is very efficient and reliable and also Quantum computing Speculative computational system that make direct use of quantum-mechanical occurrences and its work millions of time faster and provide quick response. The indication of Quantum computing is very attractive appears The quantum consequence and possibility of parallel data processing as well as the Quantum Computers prototype, demonstrates that this expertise could be used for applied application. The quantum modal of road traffic which can track the evaluation of traffic and transportable time of vehicles. Proposed modal was confirmed against the cellular automata modal. The traffic modeling contains VANET system or GPS systems. Propose modal cellular automata traffic creates a replication environment. This modal authenticate the against cellular automata modal and openhanded equivalent result.

G. Pervasive Computing and VANET

Pervasive computing is also known as a ubiquitous computing and exists anywhere. Pervasive is an emergent tendency acquaintance with microprocessor and allowing them communicate information's. Pervasive computer hypothesis the collective computing environment also imperceptible access computer systems. Pervasive computing trusts on the convergence of wireless technologies, advanced, electronics and the Internet. The basic idea of pervasive computing is gain the more power and faster results time savings and perfume the action huge amount of data. These system are the combination of collaboration among task and sentimental. Sinishibu *et al.* [12] build a modal automatic mobile that uses the pervasive computing behind the concept is use (VANET) vehicular ad- network. This paper illustrates Universal Computing for Automobiles and Methodology to Maximize User Suitability and Security Using VANETs. VANET provide the reliability and efficiency to transfer data. Data implement by using sensors and Ultra sound generator also provide the safer environment as compare to the older environment.

V. Conclusion

In this survey paper, secure VANET is essential for end user to communicate with other users and also for roadside unit (RSU). Dynamic topology and also attacker behavior make the challenges task to implement security in vehicular environment. A lot of work already done in this field and still security is challenging task for user and also for automobile industry. This paper discussed in detail the different Computing Methods and described the relationship of these methods to secure the Vehicular Ad hoc Network (VANET) from attackers and attacks. These computing methods will provide the new solutions and counter the dynamic behavior of attacker in vehicular network.

References

[1] S. Gilani, F. Shahzad, A. Qayyum, and R. Mehmood, "A survey on security in vehicular Ad Hoc networks," *Conference Paper*, 2013.

[2] R. Shringar, R. Manish, K. Nanhay, and S. Ambedkar, "Security challenges, issues and their solutions for Vanet," *India International Journal of Network Security & Its Applications (IJNSA)*, vol. 5, no. 5, 2013.

[3] N. Siddiqui, M. Shahid Husain, and M. Akbar "Analysis of security challenges in vehicular adhoc network," in *Proc. Department of Computer Science & Engineering, Integral University, Lucknow, India* ACEIT, 2016.

[4] G. Samar, A. H. Wafaa, and A. Salihy, "Security analysis of vehicular Ad Hoc networks (VANET)," *National Advanced IPv6 Center*, Universiti Sains Malaysia Penang, Malaysia.

[5] M. Newlin Rajkumar, M. Nithya, and P. HemaLatha, "Overview of Vanet with its features and security attacks," *International Research Journal of Engineering and Technology (IRJET)*, vol. 3, no. 1, 2016.

[6] R. Kruse, "Introduction to the soft computing and intelligent data analysis," in *Proc. 47th Hawaii International Conference on System Science*, Magdeburg: Rudolf Kruse Otto von Guericke University, 2014.

[7] A. Negi, K. V. Krishna, and K. Kishore, H. Kumar, "Performance evaluation of soft computing paradigms for collision detection and routing scheme in VANETs," *International Journal of Computer Science & Information Technology Research Excellence*, vol. 4, no. 3, 2014.

[8] I. Ahmed Sumra1, H. Hasbullah1, J. lail, and M. Rehman, "Trust and trusted computing in VANET," *Research Gate*, vol. 1, no. 1, April 2011.

[9] A. L. Thorp, "Attestation in trusted computing: challenges and potential solutions," *Technical Report*, 2010. [Online]. Available: http://www.rhul.ac.uk/mathematics/techreports

[10] I. Sumraa, H. Hasbullaha, J. Mananb, I. Ahmadc, and M. Y. Aalsalemd, "Trusted computing in vehicular ad hoc network (VANET)," *Computer Science Journal*, vol. 1, pp. 928-933.
[11] M. Bernas and J. Wisniewska, "Quantum road traffic model for ambulance travel time estimation," *Journal of Medical Informatics & Technologies*, vol. 22, pp. 257-264, 2013.
[12] S. Shibu1 and S. Jain2, "Pervasive computing for automobiles: An approach to maximize user convenience and safety using VANETs," *International Journal of Computer and Electrical Engineering*, vol. 2, no. 6, 2010.

Irshad Ahmed Sumra received his bachelor degree in computer science from Islamia University Bahawalpur in 2001. He pursued his M.Sc and M.S in communication and network from Bahria University Islamabad, Pakistan in 2002 -2007. Currently, he is serving as an assistant professor in Computer Science Department in University of South Asia (USA), Lahore, Pakistan. His research interest includes Intelligent transportation system (ITS), vehicular Ad hoc networks (VANET), security, big data and cloud computing.

.