A REVIEW ON AD HOC NETWORKS

Damodharan, Assistant Professor, Department of Computer Science & Engineering, Galgotias University

ABSTRACT

Ad hoc networks apart from missing infrastructure might include moving entities and different accelerations while communicating. In other words, this slows down the creation of end-to-end communication channels and increases the amount of time it takes to send data. As a result, VANETs have a range of unique network issues and security difficulties, all of which contribute to network connection, secure communications, and reputation management. This study discusses VANET security, VANET attacks, and VANET vulnerabilities, and classifies VANET assaults based on the various network levels.

KEYWORDS: VANET, ADHOC NETWORK

INTRODUCTION

The communicating entities, in this example automobiles, are ad hoc networks, and have no infrastructure or permanent resources. VANETs arise to provide services and information for passengers in a manner that offers great comfort and flexibility by letting passengers know about an emergency situation after a certain number of kilometres, for example. P2P communication may be used to apply different types of VANETs whereas multi-hop communication applies several types of VANETs. Inter-vehicle communications (IVC) or vehicle-to-vehicle communications (V2V) is also known as Vehicle-to-Vehicle communications (V2V) or Vehicle-to-Vehicle communications (V2V); its applications include monitoring and optimising a route to a destination, preventing collisions, predicting weather, and advertising goods, services, and promotions. This wide range of use gives rise to many types of phone calls these inter-related networks ITS In ad hoc networks, communication issues like interference that occur when two or more nodes attempt to connect to a single node originate from several nodes, and are sent to a single node directly. With Bluetooth and frequency hopping, the multi-hop connection is used. However, owing to the multi-hop transmission in VANETs, routing issues will occur considerably since there is no system for vehicles and nodes as part of a network architecture.

Similar to MANETs, VANETs are described as being a subset of mobile ad hoc networks. However, VANETs also differ from MANETs in that they experience fast topology changes due to rapid speeds, high likelihood of network fragmentation due to speedy vehicles, no prescribed limits on power consumption, and operation at large scales inside cities and at their outskirts. Vechicles interact with each other using specified units.

Not only does the architecture of VANETs allow for several styles, but the architecture of VANETs may also take on other styles which include cellular/WLAN (Wireless Local Area Network), ad hoc, and hybrid. The cars connect to the base stations (also known as Road-Side Units (RSUs)) or fixed distant entities to exchange and receive data (V2R Communications). The cars connect directly with one another without the need of intermediary entities (V2V communications). The previous two designs have been combined into a hybrid architecture [1]. Furthermore, automobiles in VANETs broadcast information about their speed, direction, acceleration, and traffic conditions to fixed distant nodes, such as parking metres. DSRC is a standard that arose to enable IEEE 802.11 in vehicle-to-vehicle communications. In VANETs, the FCC has allotted a 75 MHz chunk of DSRC spectrum situated at 5.9 GHz for VANETs usage. Moreover, an IEEE P1609 working group is in progress which aims to develop a standard for DSRC, the 802.11p MAC layer and the physical layer for WAVE, as described in [5].

VANET

Comfort (information/entertainment) applications, safety applications, and transport efficiency applications are the two primary kinds of applications found in VANETs [2,13]. More comfortable passenger-oriented amenities, such as traffic information systems, are linked to a passenger's need for comfort [6].

In addition to providing meteorological information, where are some petrol stations and restaurants? Safety applications focus on increasing the safety of the cars and passengers on the road; these kinds of applications rely on distant base stations and vehicle confidence (IVC). One well-known use of safety technology is providing an early warning of an emergency situation such as a flash flood crossing a roadway at a certain point[7-9]. A transport efficiency application is interested in finding the most efficient use of road traffic, while at the same time reducing vehicle crashes and traffic congestion. For the preceding use, vehicle-delivered advisory systems inform drivers about the appropriate speed to reach the green phase of a traffic system by using trustworthy base stations[8-11].

Vehicle-to-vehicle (V2V) communication, a specific feature of VANETs, shows features where vehicles communicate at varying accelerations and established communication channels among vehicles are predicated on trust relationships between vehicles. In order to achieve success for VANET applications, certain parameters must be met, such as an increase in the ratio of cars equipped with VANET tools to those that are not. Additionally, there are technical specifications to take into consideration, such as the maximum message size, how often a message has to be sent, and message latency requirements. Building a reputation management system is crucial for success in VANET applications (RMS). With this system, the relationships between cars are built, then harmful and selfish cars are separated from the network[12-14].

STRIKES IN THE VANET

It is possible for numerous assaults to impact functioning in VANETs. Some of these assaults have been performed by people who are either authorised or using malicious or compromised automobiles, while others are carried out by unauthorised or hacked cars (occurred from outsider vehicles which do not belong to a specific VANET). Additionally, these attacks can be referred to as passive attacks (the eavesdropper does not directly interact with authorised vehicles; but he can capture data as it is transmitted between them) and active attacks (where eavesdropper pretends to be a legitimate vehicle in order to redirect the path of data)[15-16].

CONCLUSION

Many studies in VANETs are in their early stages, but there is still more study to be done. Many of the current research projects have been created to deal with certain assaults, but they are vulnerable to others. In addition, special security resource consumption is required for distinct DOS assaults [17-19]. This task has much farther to go before it is finished. More research has to be done on safe routing protocols, strong key management, trust-based systems, integrated approaches to routing security, and data security at several levels. Attackers may take advantage of vulnerabilities in routing protocols to direct users to route selections of their choice or to initiate a denial-of-service attack. Jammed is one of Distributed Denial of Service (DDoS) attacks that may be stopped by utilising numerous transceivers that may be programmed to operate in separate frequency bands.

When it comes to security, cryptography is often used and it is only possible thanks to the dependable key management. In the public cryp-tography approach, the CA, regarded as a single point of failure, relies on a centralised Certificate Authority (CA). In addition to being fast, symmetric cryptography has the additional problem of the key distribution method being vulnerable to attack. In order to avoid key management issues, efficient key agreement and distribution are an active research topic in VANET [20]. Future studies should include attempts to build trust-based systems and integrate them to present defensive measures. This may be seen of as a solution to the node selfishness issue in the future. To meet the needs of finding new security risks and new defence methods, additional research is required in VANET.

REFERNCES

1. Chhabra, S., Bali, R. S., & Kumar, N. (2015). Dynamic Vehicle Ontology Based Routing for VANETs. In S. A. K. Lobiyal D.K. (Ed.), *Procedia Computer Science* (Vol. 57, pp. 789–797). Elsevier. https://doi.org/10.1016/j.procs.2015.07.477
2. Kaur, P., Bali, R. S., & Kaur, A. (2015). M-DART based Asynchronous File Sharing Scheme in VANET. In S. A. K. Lobiyal D.K. (Ed.), *Procedia Computer Science* (Vol. 57, pp. 288–295). Elsevier. https://doi.org/10.1016/j.procs.2015.07.487
3. Kumai, N., Kumar, R., & Bajaj, R. (2017). Mobile ad hoc networks and energy efficiency using directional antennas: A review. *Proceedings of the 2017 International Conference on Intelligent C*https://doi.org/10.1109/ICCONS.2017.8250662
4. Mehra, R., Bali, R. S., & Kaur, P. (2016). Efficient clustering based OLSR routing protocol for VANET. *2016 Symposium on Colossal Data Analysis and Networking, CDAN 2016*.

https://doi.org/10.1109/CDAN.2016.7570915

5. Ahram, T., Sargolzaei, A., Sargolzaei, S., Daniels, J., & Amaba, B. (2017). Blockchain technology innovations. *2017 IEEE Technology and Engineering Management Society Conference, TEMSCON 2017*, 137–141. https://doi.org/10.1109/TEMSCON.2017.7998367

6. Castillejo, P., Martinez, J.-F., Rodriguez-Molina, J., & Cuerva, A. (2013). Integration of wearable devices in a wireless sensor network for an E-health application. *IEEE Wireless Communications*, *20*(4), 38–49. https://doi.org/10.1109/MWC.2013.6590049

7. Fortino, G., Guerrieri, A., Russo, W., & Savaglio, C. (2014). Integration of agent-based and Cloud Computing for the smart objects-oriented IoT. *Proceedings of the 2014 IEEE 18th International Conference on Computer Supported Cooperative Work in Design, CSCWD 2014*, 493–498. https://doi.org/10.1109/CSCWD.2014.6846894

8. Hiremath, S., Yang, G., & Mankodiya, K. (2015). Wearable Internet of Things: Concept, architectural components and promises for person-centered healthcare. *Proceedings of the 2014 4th International Conference on Wireless Mobile Communication and Healthcare - "Transforming Healthcare Through Innovations in Mobile and Wireless Technologies", MOBIHEALTH 2014*, 304–307. https://doi.org/10.1109/MOBIHEALTH.2014.7015971

9. Han, C., Jornet, J. M., Fadel, E., & Akyildiz, I. F. (2013). A cross-layer communication module for the Internet of Things. *Computer Networks*, *57*(3), 622–633. https://doi.org/10.1016/j.comnet.2012.10.003

10. Hussain, A., Wenbi, R., Da Silva, A. L., Nadher, M., & Mudhish, M. (2015). Health and emergency-care platform for the elderly and disabled people in the Smart City. *Journal of Systems and Software*, *110*, 253–263. https://doi.org/10.1016/j.jss.2015.08.041

11. Istepanian, R. S. H., Hu, S., Philip, N. Y., & Sungoor, A. (2011). The potential of Internet of m-health Things m-IoT for non-invasive glucose level sensing. *Proceedings of the Annual International Conference of the IEEE Engineering in Medicine and Biology Society, EMBS*, 5264–5266. https://doi.org/10.1109/IEMBS.2011.6091302

12. Karafiloski, E., & Mishev, A. (2017). Blockchain solutions for big data challenges: A literature review. In K. L. Latkoski P. Cvetkovski G. (Ed.), *17th IEEE International Conference on Smart Technologies, EUROCON 2017 - Conference Proceedings* (pp. 763–768). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/EUROCON.2017.8011213

13. Nawir, M., Amir, A., Yaakob, N., & Lynn, O. B. (2017). Internet of Things (IoT): Taxonomy of security attacks. *2016 3rd International Conference on Electronic Design, ICED 2016*, 321–326. https://doi.org/10.1109/ICED.2016.7804660

14. Pang, Z., Zheng, L., Tian, J., Kao-Walter, S., Dubrova, E., & Chen, Q. (2015). Design of a terminal

solution for integration of in-home health care devices and services towards the Internet-of-Things. *Enterprise Information Systems*, *9*(1), 86–116. https://doi.org/10.1080/17517575.2013.776118

15. Petajajarvi, J., Mikhaylov, K., Hamalainen, M., & Iinatti, J. (2016). Evaluation of LoRa LPWAN technology for remote health and wellbeing monitoring. *International Symposium on Medical Information and Communication Technology, ISMICT*, *2016-June*. https://doi.org/10.1109/ISMICT.2016.7498898

16. Roehrs, A., Da Costa, C. A., Da Rosa Righi, R., & De Oliveira, K. S. F. (2017). Personal health records: A systematic literature review. *Journal of Medical Internet Research*, *19*(1). https://doi.org/10.2196/jmir.5876