Abstract

In Vehicular Ad-hoc Networks (VANET), communication can be done with mutual understanding of vehicles. This communication is an important application of Intelligent Transportation Systems. In VANET, safety of user is a main concern, for achieving this vehicles are exchanging safety messages at regular interval to increase the passenger safety on road. But similar to other technology VANET is also suffering from some noticeable issues. From these issues one of the most important issues is security. Since the network is open and accessible from everywhere in the radio range of vehicle nodes, it is expected to be an easy target for malicious users. The availability of the network is extremely needed when a vehicle sends any safety information to other one. In this regard, Denial of Service (DoS) with spoofed IP attacks are very dangerous in VANET because they adversely affect the network availability and very difficult to detect. Oppress the node resources by flooding of messages to the victim vehicle is one of the most dangerous type of DoS attack, in which a malicious node sends a large number of message to the victim node and because attacker uses different ids for doing it, so it is very difficult for a victim to identify that sender of massages is a attacker or a legitimate VANET user.
In this paper, we propose a Neighbor Trust Algorithm (NTA) which is an efficient method to
defend against Denial of Service attack (DoS) with Spoofed IDs attacks.

References

   prevention to DoS attacks in VANET," Contemporary Computing (IC3), 2014 Seventh
   International Conference on, Noida, 2014, pp. 270-275. doi: 10.1109/IC3.2014.6897185
2. Lyamin, Nikita, Alexey V. Vinel, Magnus Jonsson, and Jonathan Loo. “Real-Time
   Detection of Denial-of-Service Attacks in IEEE 802.11 pVehicular Networks”, IEEE
   foundations for the design of a low-rate DoS attack to iterative servers (short paper)” Lecture
   cost tradeoffs for vehicular access networks” IEEE Transactions Intelligent Transportation
5. Spaho E., Ikeda M., Barolli L., and Xhafa F. “Performance Evaluation of OLSR and AODV
   protocols in a VANET crossroad scenario” in proceeding of the IEEE 27th Advanced Information
6. Biswas S., Misic J., and Misic V. “DDoS attack on WAVE-enabled VANET through
   synchronization” in proceeding of the IEEE Globalcommunications conference, pp. 1079-1084,
   3-7 Dec. 2012.
7. Zeadally, Sherali, Ray Hunt, Yuh-Shyan Chen, Angela Irwin, and Aamir Hassan.
   “Vehicular ad hoc networks (VANETS): status, results, and challenges”, Telecommunication
8. Karagiannis, Georgios, Onur Altintas, Eylem Ekici, Geert Heijenk, Boangoat Jarupan,
   Kenneth Lin, and Timothy Weil. “Vehicular networking: A survey and tutorial on requirements,
   architectures, challenges, standards and solutions”, IEEE Communications Surveys & Tutorials,
   2011.
   (dos) attack and its possible solutions in VANET.”, World Academy of Science, Engineering and
10. José María de Fuentes, Ana Isabel González-Tablas, Arturo Ribagorda, “Overview of
    security issues in Vehicular Ad-hoc Networks”, Handbook of Research on Mobility and
    Computing 2010.
11. Studer A., Bai F., Bellur B., and Perrig A “Flexible, extensible, and efficient VANET
    authentication” Journal Communications and. Trans. Networks, vol. 11, Issue 6, pp. 574-588,
    comparative study of mobile and vehicular adhoc networks” International Journal Recent Trends
    Yan, Stephan Olariu, Michele C. Weigle, “Providing VANET Security through active position
Neighbor Trust Algorithm (NTA) to Protect VANET from Denial of Service Attack (DoS)


Index Terms

Computer Science Wireless

Keywords

Neighbor Trust Algorithm (NTA), Denial of Service (DoS) Attacks, DSRC (Dedicated Short Range Communication).