HiLL PUBLISHING

Engineering Advances, 2022, 2(2), 175-181
https://www.hillpublisher.com/journals/ea/
ISSN Online: 2768-7961

Research on the Characteristics and Detection Methods of DDoS Attacks on Wireless Sensor Networks for Vehicle Networking

Xiaofen Fang[1], Kunli Fang[1], Guohua Li[2], Xinjun Jin[1,*], Lihui Zheng[1]

[1]School of Mechanical and Electrical Engineering, Quzhou Vocational and Technical College, Quzhou 324000, China.
[2]Quzhou Haixi Electronic Technology Co., Ltd, Quzhou 324000, China.

How to cite this paper: Xiaofen Fang, Kunli Fang, Guohua Li, Xinjun Jin, Lihui Zheng. (2022) Research on the Characteristics and Detection Methods of DDoS Attacks on Wireless Sensor Networks for Vehicle Networking. *Engineering Advances*, 2(2), 175-181.
DOI: 10.26855/ea.2022.12.006

Received: November 20, 2022
Accepted: December 18, 2022
Published: December 30, 2022

***Corresponding author:** Xinjun Jin, School of Mechanical and Electrical Engineering, Quzhou Vocational and Technical College, Quzhou 324000, China.

Abstract

Smart vehicles constitute the intelligent transportation system, the complex traffic network of multiple types of sensors in the energy consumption data and the amount of data transmitted is increasing, the network consisting of multi-source wireless sensors in the vehicle is often subject to DDoS attacks, the DDoS will lead to data loss or even traffic failure. Since multiple distributed vehicle nodes are dynamic constantly entering or leaving a network cluster, as smart vehicles continue to join the new wireless sensor network and obtain new identity IDs based on location, IP addresses are always allocated and recycled. DDoS attacks against vehicle networking clusters are difficult to identify, destructive and easy to implement. In this paper, we analyze the topology and communication patterns of wireless sensor networks in vehicular networks, the characteristics of being subject to DDoS attacks, the detection methods of each, and propose the initial detection and energy consumption trust value calculation for the detection of DDoS attack network nodes.

Keywords

Wireless sensor network, DDoS attack, Vehicular network

1. Introduction

Wireless sensor network through the "end" - sensor nodes to collect electromagnetic, temperature, humidity, vibration, image, audio, video and other information data, and a variety of information data in the network for integrated processing. In the entire wireless sensor network, the sensor nodes without tamper-proof in the open environment, some even in the remote and harsh environment, and its dynamic changes in the network, resulting in a series of wireless sensor network attacks such as Sinkhole, wormhole, Sybil.

Wireless sensor network security includes active and passive attacks, active attacks are listening through unauthorized communication channels and thus tampering with the data flow information in the communication channels; passive attacks are collecting sensitive data through hidden "nodes" through communication lines [1]. There are many network security in wireless sensors such as message authentication, intrusion monitoring, and access rights. DDoS (Distributed Denial of Service) utilizes a large number of legitimate distributed servers to send requests to the target computers, resulting in the inability of normal legitimate users to obtain services. The first DDoS attack- Panix Attack occurred on September 6, 1996. As computer performance improves, target computers are attacked as DDoS, taken simple method just throughing the SMTP port of the target object. The attackers continues to send a large number of connection requests to the server, and the server is difficult or cannot responding to normal users. In addition, the attackers have resorted to immediately spoofing the source IP to make the source difficult to trace. It is currently one of the most problematic network security issues in wireless sensor networks.

Currently there are more monitoring methods proposed for DDoS attacks on wireless sensor networks at home and abroad, With the wide application of wireless sensors in Vehicular Ad hoc Networks (VANET), the network topology composed of wireless sensors within VANET shows dynamic changes because the vehicle itself is in a driving and moving state. In the future ITS, network security will be the most important part, Batchu et al. [2-4] used Semi-supervised machine learning obtaining subsets of unlabeled or partially labeled dataset based on the applicable metrics of dissimilarity. Singh et al. [5-7] used two stages model that the optimal features were subjected to classification using the Deep Convolutional Neural Network (CNN) model, in which the presence of network attacks can be detected. A bait detection mechanism is launched in second stage, which provides the effective mitigation of malicious nodes having Distributed Denial-of-Service (DDoS) attacks.

In summary, as future vehicles are further intelligent, as well as the development of intelligent driving, vehicles no longer include only pressure sensors, position sensors, temperature sensors, acceleration sensors, and angular velocity sensors, while equipped with intelligent sensors such as lidar, millimeter wave radar, ultrasonic radar for environmental sensing, the vehicle internal sensors wireless self-organization of the way to form multiple nodes sensor network , vehicles, vehicles and roadside infrastructure units between the same time also formed a multi-node, multi-dimensional wireless sensor network. As the wireless sensor network itself is vulnerable to network attacks and tampering, reducing the stability and security of the entire intelligent driving traffic network composed of smart cars, real-time continuous monitoring of the behavior and performance of the nodes in the network to assess the trust value of the nodes to improve the security of the network is not only computationally intensive but also consumes excessive network energy resources. DDoS attacks characteristics, in the intelligent driving traffic network, for wireless sensor networks to propose the corresponding attack detection method.

2. Network topology and assumptions

2.1 Network topology

According to the characteristics of the network constituted by sensors equipped with intelligent vehicles, it is divided into three levels of network constituted by internal vehicles, external vehicles together, and wireless sensors with external traffic systems.

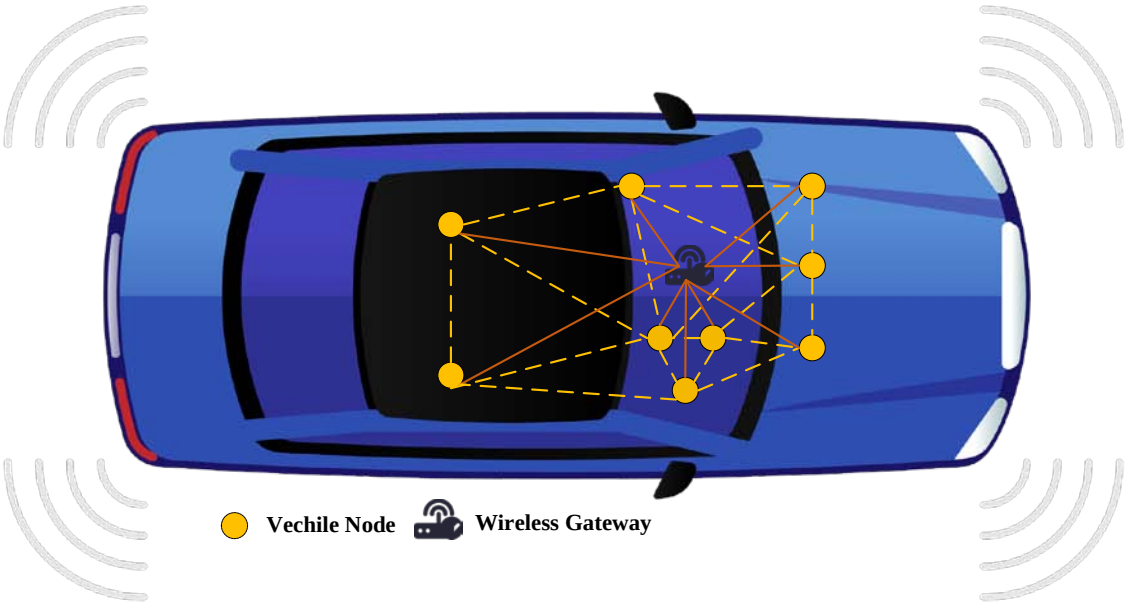

Figure 1. Clustering topology of wireless sensors in the vehicle.

The wireless sensors inside the vehicle are centered on the wireless gateway and form a cluster topology as shown in Figure 1. The node positions in the wireless sensor network are fixed, and the sensors at the same level can communicate with each other. As the current network inside the vehicle is using bus type, the data collected by various sensors need to pass through the gateway, and the future of the smart car inside the increased use of wireless sensors for (P2P, Peer to Peer) self-organizing network.

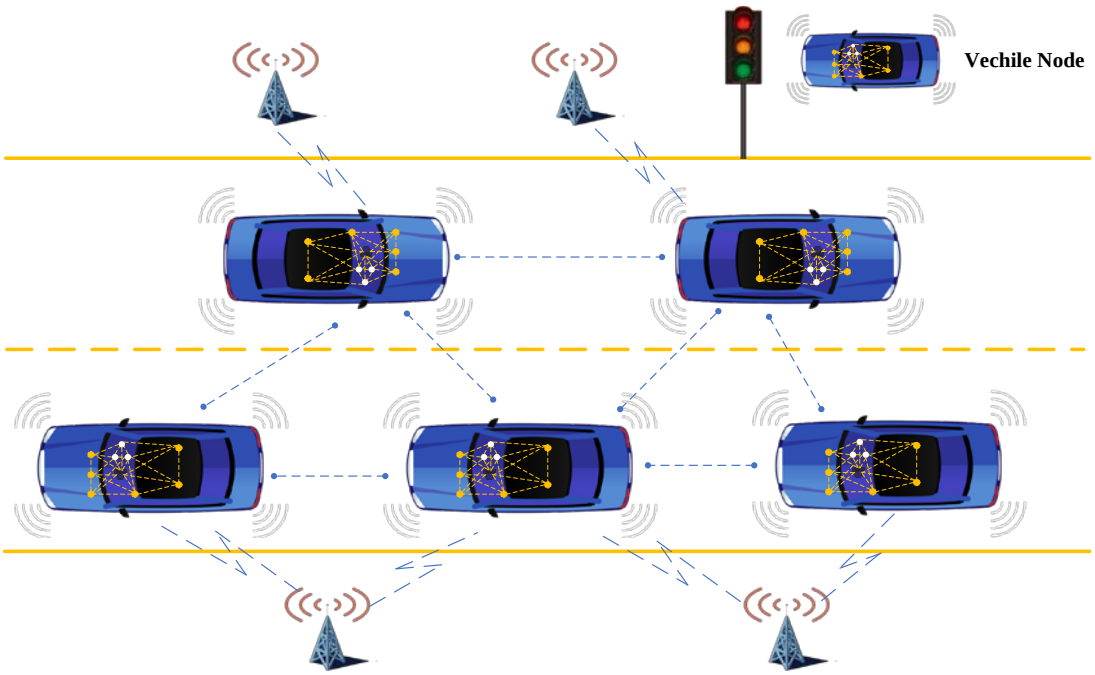

Figure 2. Topological diagram of vehicles as network nodes in an intelligent transportation system.

The wireless communication network formed between vehicles and vehicles, vehicles and roadside infrastructure unit RSUs during the operation of smart vehicles on the road, as shown in Figure 2. Among them, the roadside infrastructure unit RSU includes the base station, and the smart vehicle wireless gateway is on the road as a network node, constantly regrouping itself, and constantly disconnecting and self-grouping with the roadside infrastructure unit RSU. The topology of the network composed of its wireless sensors is dynamically changing over time, and the network nodes are with bidirectional data exchange between nodes.

2.2 Two-way communication model

There is bi-directional mutual communication of data between network nodes in wireless sensor networks.

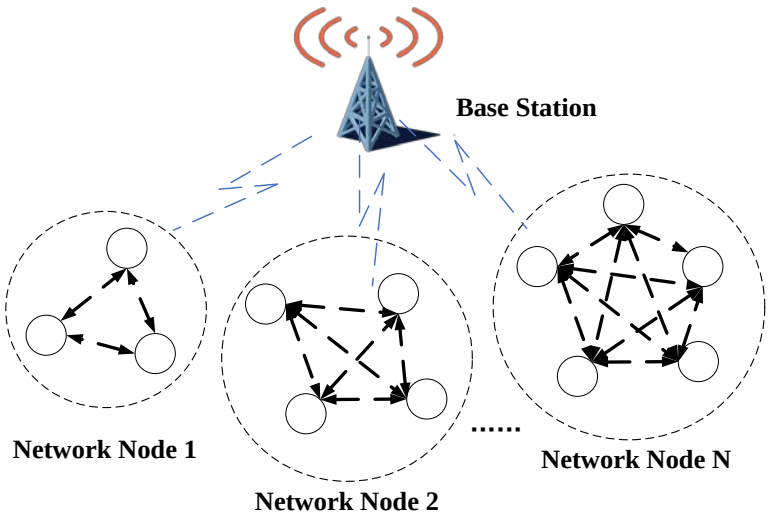

Figure 3. Two-way communication model in Wireless Sensor Networks.

As there is a local area network of wireless sensors inside the smart vehicle, connected by a smart wireless gateway. When the vehicle is in motion, the whole LAN is mobile and capable of two-way data communication with the base

station, as shown in Figure 3.

3. Telematics DDoS attack features

DDOS attacks generally mean that attackers use "broilers" to launch a large number of requests to the target website in a short time, consuming the host resources of the target website in a large scale, so that the target server is paralyzed and cannot be accessed.

(1) Distribution. DDoS attack is a cooperative attack launched against the victim host through the joint or control of several attackers distributed in different locations. The distributed feature not only increases the attack strength, but also makes it more difficult to resist attacks.

(2) Fraudulence. Falsifying the source IP address can achieve the purpose of hiding the attack source, while the common attack source location technology is difficult to trace this attack. Accurately locating the attack source is the key to identify the forged source IP. Most of the current IP location technologies can only locate the attack network boundary router or proxy host.

(3) Invisibility. For some special attack packets, their source address and target address are legal. For example, in an HTTP Flood attack, you can use the real IP address to launch a DDoS attack.

(4) Extensive destructiveness. DDoS attacks use a large number of puppet hosts to attack the target host at the same time, and the attack flow may become very large after multi-party aggregation. In addition, because of its characteristics of distribution, concealment and deception, it can not only avoid the conventional defense system, but also cause serious economic losses.

3.1 Identity ID and location information

Identity ID and entity node location one-to-one correspondence are the basis for the normal operation of the network. Within the smart vehicle, different wireless sensor networks appear as spoofed nodes, and once a sensor node is attacked by Sybil, the whole system is seriously damaged due to the spoofed node misjudging the location information and status information of the normal nodes by sending the wrong information to the other nodes of the wireless sensor. For example, after the smart coolant temperature sensor is attacked by DDoS, the disguised smart coolant temperature sensor node will enter in inoperable state in the network, which leads to the whole network system making judgments based on the blank information.

Smart vehicle sensor nodes only collect data inside the vehicle, and the smart gateway constitutes a sensor wireless network with a limited number of nodes, a fixed network topology, a limited collection range, a controlled communication range, etc. The ID of the forged new identity is often easier to identify and judge, so DDoS attacks are usually a large number of false request data to occupate of network computing capacity.

For intelligent vehicles in the process of moving, the location of the vehicle relative to the adjacent vehicles, and by multiple intelligent vehicles constitute a wireless network and then communicate with the base station, intelligent vehicles relative to the base station is mobile. The network nodes are in a state of change, resulting in frequent changes in network topology over time. DDoS attacks are difficult to be identified when network nodes in mobile state. As smart vehicles continue to join the new wireless sensor network, the need to obtain new identity IDs based on location, then in this dynamic change process, DDoS nodes are difficult to be identified and detected. It leads to the misjudgment of the whole intelligent transportation network so that the system is paralyzed.

3.2 DDoS Attack method

Sybil attacks include SYN Flood, ACK Flood, UDP Flood, ICMP Flood, TCP Flood, Connections Flood, Script Flood, Proxy Flood, etc. For example, one of the most effective DDOS attack methods, the SYN Flood method uses the principle of TCP protocol to attack. By sending a large number of SYN or ACK packets forged source IP and source port to the victim host, the host's cache resources are exhausted or the host is busy sending response packets, resulting in a denial of service.

In SYN Flood method, before the TCP channel is established, three handshakes are required:

(1) The client sends a TCP message containing the SYN flag. The synchronization message indicates the port number required by the client and the initial serial number of the TCP connection.

(2) After receiving the TCP message, the server returns a SYN+ACK message, indicating that the client request is accepted, and the TCP initial serial number is increased by 1. The client returns an ACK message to the server, and the TCP serial number is also increased by 1.

(3) If the server does not receive ACK from the client, it is in the waiting state. Add the client IP to the waiting queue, and then continuously send SYN+ACK messages.

Vehicles are in motion on road, when one vehicle enters a network cluster, it dynamically obtains an IP address. When it produces DDoS attacks on other nodes, it is difficult to identify its specific location. If it continuously sends

huge messages to the RSU, the RSU is paralyzed and will no longer serve other vehicles.

4. Testing Method

4.1 Initial testing

To detect node identity ID inconsistencies in wireless sensor networks, as well as static position information Position, node state with abnormalities under the data collection moment Time, static position information Position abnormalities are calculated.

$$d_x = P_x - \bigcap_{i=1}^{j}(P_i, r_i)$$

Where, at a certain moment t, Px is the spatial location where a certain intelligent vehicle node is located, Pi is the spatial location where the ith intelligent vehicle in the network cluster is located, ri is the effective communication radius of the ith intelligent vehicle, dx is the distance of a certain intelligent vehicle from the center of the network cluster, and exceeding the threshold value, the node position information Position is judged to be abnormal.

When the intelligent vehicle node ID is the same, but at the moment of t data collection, and in the network cluster within the static position information Position of the same road section, a vehicle state data State (speed, coolant temperature, engine speed, etc.), the difference value with the neighboring vehicles in the same network cluster exceeds the threshold, then it is judged that the intelligent vehicle node has been attacked by DDoS, and its generated data packets will be discarded.

4.2 Energy consumption trust value calculation

The energy consumption trust value is based on the calculation of the energy consumption trust value of network nodes based on the forged legitimate node identity ID and static location information Position after the Sybil attack in the vehicular network, i.e., the relationship between the remaining energy Eres and its initial energy E0 for each network node.

$$E_0 \geq E_{res} + E_{avg} + \tau$$

E_{avg} The average energy already consumed by all member nodes in the network cluster where the current network node is located, τ is the energy replenishment value, which is adjusted according to the working conditions where it is located.

The task of detecting DDoS attacks based on intelligent vehicle network nodes, where the specific algorithm implementation steps are shown in Table 1.

Table 1. Intelligent vehicle network node detection of DDoS attack

Detection of DDoS attacks by intelligent vehicle network nodes.
Input: *ID, Position, Time, State, port*, E_{res} and gateway fusion data
Output: Identify node DDoS attacks in the network
Algorithm: (1) The base station receives the intelligent vehicle network node gateway packets; (2) The base station detects the initial detection by the ID and Position of the smart gateway; If CH(*ID*, *Position*, *Time*, *State*, *port*) match *R*, then (3) If $E_0 \geq E_{res} + E_{avg} + \tau$, then (4) *S*++; (5) Else (6) *U*++; (7) If T (Δt)$\geqslant$10 then (8) The base station accepts gateway packets from this network node; (9) Else (10) Go to step (13); (11) Else (12) There is a DDoS attack that drops the sent packets; (13) End

4.3 Comparison of different layers of DDoS attack detection

In the vehicular network, different levels of wireless sensors constitute a network with different complexity and topology, and face different characteristics of DDoS attacks, and the strategies adopted for different levels of DDoS attacks are also different [6-7]. According to the three levels of intelligent vehicles internal, vehicles, and traffic systems are divided, as shown in Table 2.

Table 2. Comparison of DDoS attack detection in different levels of networks

Node Composition	Attack Difficulty	Detection Difficulty	Level
Consists of intelligent sensors in the vehicle, location, number fixed, bus type communication	Easy	Easy	L1
By the intelligent vehicle as a network node, location, number of large changes, mesh type	Easy	Hard	L2
By the base station and intelligent vehicles constitute a network cluster for interaction, one side moves, relative position, number is not fixed	Easy	Hard	L3

Since smart vehicles contain 60 to 100 sensors, there is a high degree of coupling, cohesion between the CPS components (sensors, devices, systems) of the vehicle. Multiple layers of interaction between the sensing, communication, and control layers, and cyber attacks in the sensing or communication layers can compromise the security of the control layer, especially for vehicle dynamics sensors (tire pressure monitoring systems (TPMS), magnetic encoders, and inertial sensors) and environmental sensors (e.g., light detection and ranging (LiDAR), ultrasound, cameras, radio detection and ranging systems (radar), and global positioning systems (GPS)) are more prominent. In connected vehicle systems, it is therefore crucial to detect and identify attacks quickly and effectively against wireless sensor networks consisting of smart vehicles as network nodes.

5. Summary

This paper presents the intelligent vehicles constitute the intelligent transportation system, vehicles by the vehicle network connection communication, analysis in the wireless sensor network DDoS attack characteristics. Since multiple distributed vehicles are in motion, and vehicles are constantly entering or leaving a network cluster, IP addresses are always allocated and recycled. Its attacks against network clusters are difficult to identify, and are covert, destructive and easy to implement. Once attacked, it is difficult to recover in a short time. In the Internet of Vehicles, if abnormal traffic is cleaned and filtered through the DDoS hardware firewall, the rule filtering of data packets, fingerprint detection filtering of data streams, and customized filtering of data packet content often lead to a decline in network speed. The intelligent transportation system has a high demand for network speed and computing capacity. The two-step strategy of identifying location and ID first, and then energy consumption will be more advantageous. Fusion of preliminary detection and energy consumption trust value calculation methods for different levels of DDoS attacks and detection were compared and analyzed, intelligent vehicles in the intelligent transportation system to operate safely and efficiently, the full lifecycle security of traffic data will face serious challenges. In the subsequent work, other attacks and vulnerability detection in the intelligent transportation system that threaten the security of traffic data will be in-depth.

Acknowledgements

This work was support by the Quzhou city guiding science and technology research project: Research on key technology of wireless sensor network attack detection for intelligent driving (No.2021069). Project of university-enterprise cooperation for domestic visiting engineers in colleges and universities: Research on key technology of pure electric vehicle drive system state monitoring based on big data (FG2019163).

References

[1] Aamir, M., Zaidi, M.A. (2021). Clustering based semi-supervised machine learning for DDoS attack classification. J. King Saud Univ. Comput. Inf. Sci., 33, 436-446.DOI:10.1016/J.JKSUCI.2019.02.003.

[2] Batchu, R., & Seetha, H. (2021). A generalized machine learning model for DDoS attacks detection using hybrid feature selection and hyperparameter tuning. Comput. Networks, 200, 108498. DOI:10.1016/j.comnet.2021.108498.

[3] Aamir, M., Zaidi, M.A. (2019). DDoS attack detection with feature engineering and machine learning: the framework and per-

formance evaluation. International Journal of Information Security, 1-25. DOI:10.1007/s10207-019-00434-1.

[4] Marvi, M., Arfeen, A., & Uddin, R. (2021). A generalized machine learning‐based model for the detection of DDoS attacks. International Journal of Network Management, 31.DOI:10.1002/nem.2152.

[5] Singh, S., & Jayakumar, S. (2022). DDoS Attack Detection in SDN: Optimized Deep Convolutional Neural Network with Optimal Feature Set. Wirel. Pers. Commun., 125, 2781-2797. DOI:10.1007/s11277-022-09685-z.

[6] Behal, S., & Kumar, K. (2017). Detection of DDoS attacks and flash events using novel information theory metrics. Comput. Networks, 116, 96-110. DOI:10.1016/j.comnet.2017.02.015.

[7] Alrehan, A.M., & Alhaidari, F.A. (2019). Machine Learning Techniques to Detect DDoS Attacks on VANET System: A Survey. *2019 2nd International Conference on Computer Applications & Information Security (ICCAIS)*, 1-6. DOI:10.1109/CAIS.2019.8769454.