THINK INDIA JOURNAL

ISSN: 0971-1260
Vol-22-Issue-16-August-2019

Security Constraints, Solutions and IDS In Vehicular Network: A Review

Dipta Datta[1], Chavi Kapoor[2]
[1,2]Lovely Faculty of Technology and Sciences
Lovely Professional University, Punjab, India
[1]diptadatta81@gmail.com, [2]ch.kapoor01@gmail.com

Abstract-Vehicular ad-hoc network (VANET) has become one of the fast-growing topics in the modern wireless network. VANET has introduced the advancement system for the vehicular nodes. Using different modern applications and methods, VANET has brought revolutionary changes in the road traffic system. With the advancement of the network, VANET has different security issues. Unique features and fixed resources make the security design a difficult task. Attackers use different attack techniques to compromise the network. Any attack in the network may cause big accidents or huge data loss. So, security is a major and important part in VANET. In this paper we introduce the security challenges with proper solutions. We also explain different attacks and try to focus on the solutions for the attacks. Intrusion detection system (IDS) and its different model with features for VANET are also given in this paper.

Index terms- VANET, IDS, OBU, RSU, attack, security challenges.

1. INTRODUCTION:

VANET is now very popular ad-hoc network for its rapid growth with the modern era. To develop Intelligent Transportation System (ITS), VANET is the most important part. VANET gathers different important information about other vehicular nodes to avoid any danger. VANET usually uses the mobile ad-hoc network (MANET) and flying ad-hoc network (FANET) to establish the connection and to gather the data from other nodes. That means VANET is playing a very important role in the safe vehicular system. But security is a major issue in VANET. Vehicular nodes exchange different important and sensitive information through the networks. But any type of unwanted outside attack can make a big loss of the information. Any unauthorized node can perform different malicious activities such as corrupting data, leaking data, dropping data, modifying data, etc [1].IDS is one of the suitable solutions for such traditional networks for ages and provides effective ways to deal with network intrusions.

In this modern era, with the rapid development of technologies, different modern sensors and security model are using to manufacture the vehicular nodes. Different sensors sense the nearby obstacles and inform to the drivers. But different vehicular nodes have different designs. As a result, all nodes cannot

ISSN: 0971-1260
Vol-22-Issue-16-August-2019

sense all these different types of obstacles. VANET has given solution to this problem. The main motto of VANET is to provide proper safety and to reduce accidents. To provide proper data about the other vehicles VANET has two units; roadside units (RSUs) and on-Board units (OBUs) [2]. RSUs are the roadside access points that are used to transfer the data. RSUs monitor the traffic and collect data about single and multi-lane free roads. OBUs are the installed units that communicate with the RSUs. The OBUs get connected to a dedicated short-range communication (DSRC) wireless network [3]. The RSUs are connected to the control stations through the ground base-stations (GBSs) or ethernets (Figure: 1).

Though VANET is providing a promising safety from any accident, it is very hard to design a security architecture for VANET; because VANET is a wireless network. Any unwanted malicious node can be involved in the network to make damage to information. The unwanted malicious node can interrupt the transmission, damage the data, modify the information. As a result, the main purpose of the network will remain unfulfilled. So, a secure and efficient design is the major constraint in VANET. To provide suitable security many researchers addressed different security designs. Among those designs, IDS has gained the most popularity by detecting malicious nodes easily. But it is not easy to apply IDS in VANET because of the particular characteristics. Because IDS needs high computation and large storage capacity to detect malicious nodes quickly and the nodes of VANET don't have that much resources [4]. That's why the deployment of IDS in VANET is a challenging issue. Again, the high mobility and frequently changing positions are also the major constraints in deploying IDS in VANET.

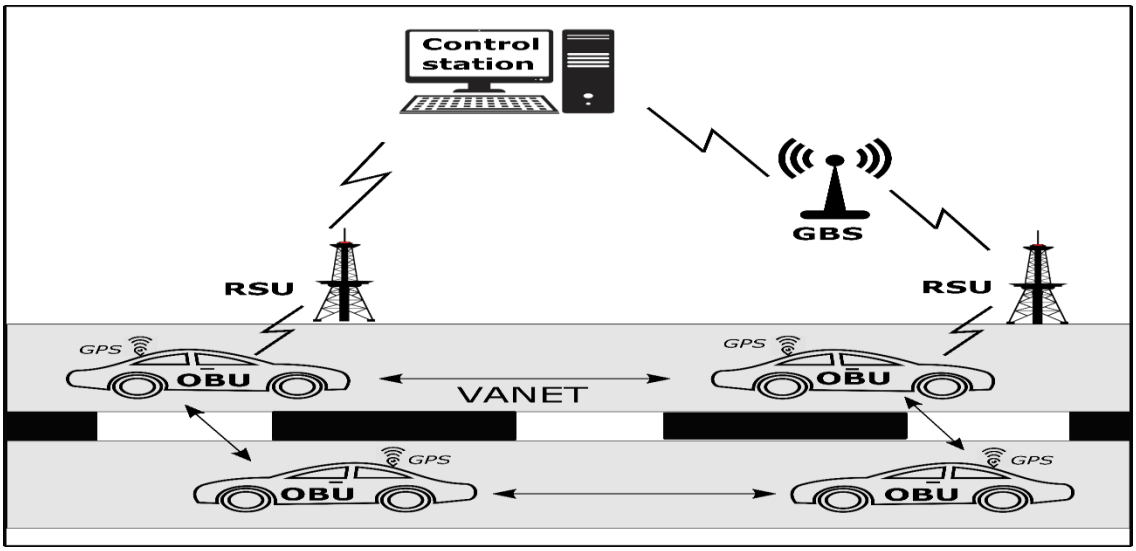

Figure 1: General VANET design

ISSN: 0971-1260
Vol-22-Issue-16-August-2019

2. RELATED WORKS:

As VANET is now-a-days one of the popular wireless networks, many researchers have given different security and efficient models to maintain the safety of the network.

Sharma and Kaul [1] presented a brief knowledge of IDS in VANET for proactive security mechanisms. They tried to develop IDS for VANET to get potential outputs. They also addressed a honeypot based proactive security mechanism to detect different attacks. They also tried to improve the detection mechanism to detect zero-day attack and to minimize the overhead.

Dow et. Al [2] proposed a model for VANET that collects real-time traffic data and gives warning with notifications. This model is capable to detect traffic information using DSRC and can transmit the information through the network. They also provided a model to maintain the network and the model can gather the self-check data to transmit to the cloud [2].

Bai and Krishnan [3] used vehicle-to-vehicle transmission data to analyze the link-levelbehavior of the DSRC network. They developed a model for application level to provide vehicular safety. They related DSRC communication with vehicle safety communication (VSC) to provide proper security for the network.

Loukas et. Al [5] tried to give a solution for the limited processing resource issue in VANET. They used different resources to gain real-time data related to cyber and physical processes. Using deep learning, they tried to address a reliable network with the help of physical IDS.

Ali Alheeti et. Al [6] represented anintelligent IDS model to anomaly detect grey hole and rushing attacks. This model can also detect malicious behaviors in the network. They analyzed that their model gave a better detection rate and reduced fake alarms.

Al-Jarrah et. Al [7] gave a complete overview of IDS in an intra-vehicle network. They provided a general overview of the intra-vehicle network and then used IDS to gave proper security. They analyzed different methods to give proper compression. They also explained different challenging issues of IDS based intra-vehicle network.

Sedjelmaci et. Al [8] addressed a light-weight and efficient IDS model for VANET. The purpose of the model was to detect denial-of-service (DoS), integrity target and fake alert attacks.This model can detect malicious nodes with high accuracy. The high detection rate and the low false-positive rate made the model a proper solution for VANET.

ISSN: 0971-1260
Vol-22-Issue-16-August-2019

Zaidi et. Al [9] provided a model of host-based IDS in VANET to detect false notification attacks in the network. They addressed a theory to train IDS for the network. The model used statistical methods to detect the malicious nodes in the network.

Sangve et. Al [10] proposed a model where IDS is used in VANET to detect false notification attack. They used anomaly-based detection method for rogue nodes to get better detection accuracy. All nodes transfer the meta-information from RSU and calculate the data for further transmission.

Sakiz and Sen [11] explained different attacks and possible security mechanisms of VANET. They addressed different attacks with their effects and provided solution with proper advantages and disadvantages. Different challenging issues of VANET with different ideas of solutions are also addressed in their paper.

3. SECURITY CHALLENGES OF VANET:

The high mobility and density with fixed resources are the main reasons for having different challenging issues in VANET. The specific characteristics of VANET are the major reasons for the issues. These characteristics also make the design very hard and give easy access to outside attacks. These specific features of VANET are responsible for the following challenging issues:

Privacy: It is not easy to provide a proper security model along with the privacy model in VANET. Normally, every driver wants to protect their information about their locations and histories [12]. As a result, the controller cannot get information about any occurrence on the road. Here, providing privacy is the main constraint for the security model. To handle all the vehicles, one model needs to be implemented that ensures providing critical traffic information though the drivers don't want to share all information.

Mobility:The nodes of VANET moves very fast and change their location frequently. While moving with over 20m/s speed [13], it is not easy to stay connected with the network for the nodes. As a result, packet loss and link breakage happen. In this position, it is not easy to provide a proper security model for VANET.

Scalability: VANET has high density. There are over 250 million vehicles connected with VANET worldwide [14]. There is no standardized rule to give proper security for the huge number of nodes. Normally different local and private authorities are trying to provide security for a limited area. As a result,

ISSN: 0971-1260
Vol-22-Issue-16-August-2019

the traffic information of outside of the area can not be included in the network and drivers cannot get informed about any occurrence of those places while driving.

Limited resource: The other major challenging issue of VANET is the limited resource. As VANET have fixed resources, the implementation of security within the limited resources is a difficult task.

Except these following reasons, VANET has other different reasons for having security constraints. Generally, IDS is used to give protection to VANET. But, if an attack happens in the network, the network system must need to take immediate decisions to tackle the incident.Here in the network IDS sends notifications or alerts the drivers about the incident to take manual actions. Here, drivers may not have the proper knowledge about the proper actions during the incident. This may cause a big loss in the network. the attacker gets more time to corrupt the data of the network.

Normally, RSUs can not be installed everywhere because of cost management. So, all OBU devices can not be connected to the RSUs all the time. Though OBU devices can be connected with other OBU devices to share information, all devices may not be connected with the RSUs. As a result, any middle attack where RSU is absent can happen. In this situation, OBU devices may not get access to the control stations. It occurs a big packet loss and data breakage.

4. DIFFERENT ATTACKS IN VANET:

With the advancement of wireless networks, the ideas of attackers are also getting advanced. When attackers get any leak in the network, they try to attack the network with different types of attacks. So, security is a big concern for any network. In VANET attackers use special techniques to attack the network. Attackers try to use the network for their own purpose for their easy travels. They also attack the network to make accidents and roadblocks.

4.1. Sybil attack:

Sybil attack is one of the dangerous attacks in VANET. Sybil attack creates a scenario where specific nodes get multiple identities. That means attackers attack any node and gather its information and broadcast the information for multiple places. As a result, the normal nodes think that there are multiple nodes and change their direction for an easy journey. For example, an attacker provides fake information in the network about the road that the road is congested and blocked so that the other nodes change their direction to other routes (Figure:2). The nodes whose identities are stolen are called Sybil nodes and the attacker node is called Sybil attacker. Sometimes Sybil attack can make a big accident and this attack

ISSN: 0971-1260
Vol-22-Issue-16-August-2019

cannot be detected easily [15]. It is very difficult and takes a long time to detect Sybil attack and so Sybil attack is a very dangerous attack.

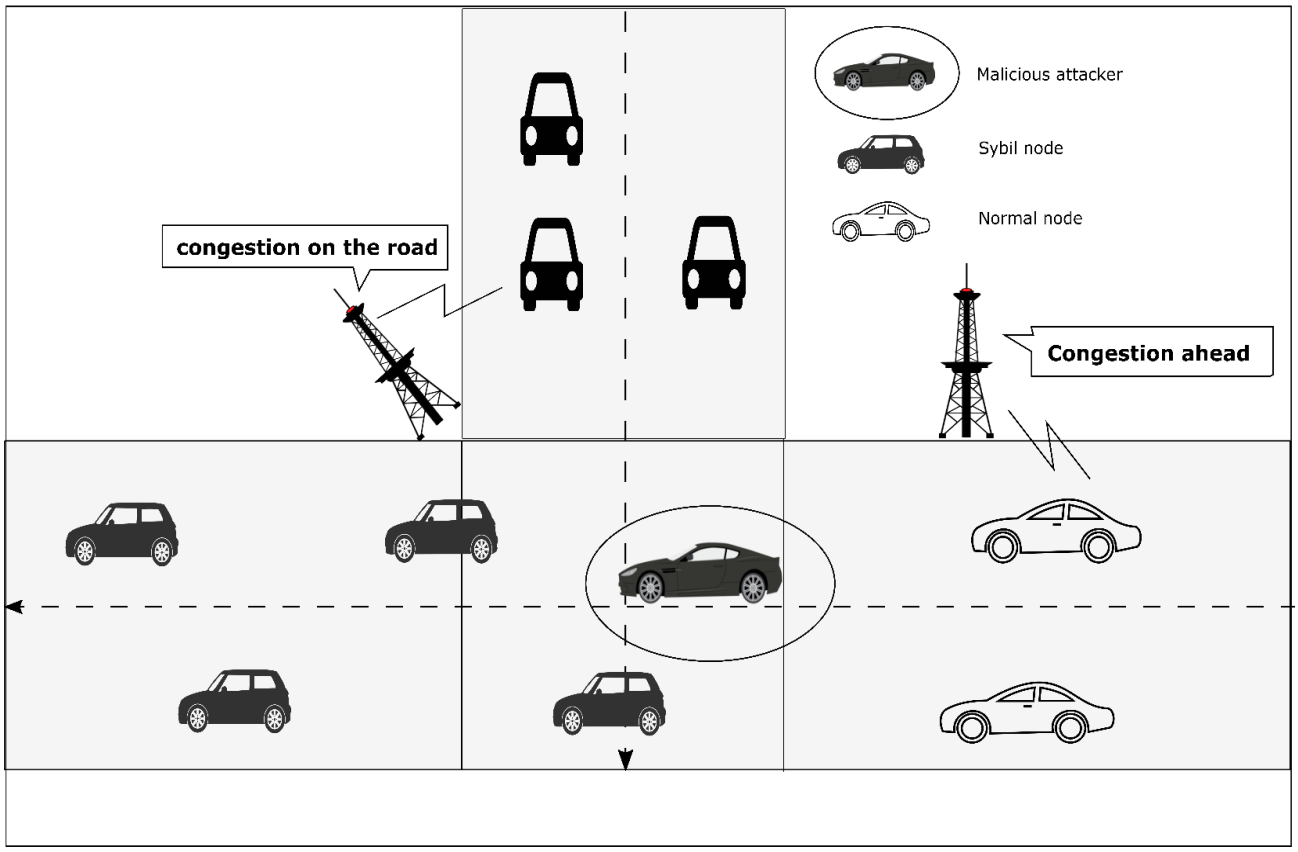

Figure 2:Sybil attack

Sybil attack is also known as an identity spoofing attack. Because attackers spoof the identities of the nodes to make illusion in the network. Then attackers can inject fake information in the VANET cloud. This can make a big accident on the road. For example, if there occurs any accident, the nearby vehicle will send the message to other nodes and other nodes to the network. If there is an attacker on the road and the attacker receives the message about the accident and does not forward the message further and also modifies it, then there may occur a big accident. Sybil attack has three categories [16].

a) **Identity theft category:** In the Sybil attack, an attacker steals identities of nearby nodes. Then they use the identities to create illusions on the road to mane congestion on the road. Attackers can steal identities of random nodes (random identity theft) or nearby legitimate nodes (legitimate identity theft).
b) **Communication category:** when there is a Sybil attacker in the network, any normal node may transfer messages to the Sybil nodes. When Sybil nodes get the massages, they pass them to the

ISSN: 0971-1260
Vol-22-Issue-16-August-2019

Sybil attacker. Then the attacker can modify or change the data of the massages. When normal nodes directly send data to the Sybil nodes then it is called direct communication. And when normal nodes send data to the Sybil nodes through Sybil attacker then it is called indirect communication [1].

c) **Participation category:** Sybil attacker uses the spoofed identities to make one or multiple fake identities to make congestion on the road. The fake identities make the other normal node confused and create congestion on the road.

4.2. DoS attack:

DoS attack is a common attack in every network. DoS attack makes the network freeze for a time. As a result, other nodes can not use the network. In this attack, attacker continuously sends requests to the network system so that the system can not handle all the requests. Thus, attacker makes the system shut down for a time. Within the time, other nodes can not share or receive any type of data through the network. Flooding attacks [11], JellyFishattack [17] and intelligent cheater attack [18] are different types of DoS attack. In data flooding attacks, attackers share useless data in the network again and again to make the network busy with useless requests. JellyFish attack normally attacks the protocols of the network and makes the system disordered and creates a delay in the network. Intelligent cheater attack also attacks the protocols and continuously tries to make the network having misbehaves to the other nodes. Both of the attacks are difficult to detect.

4.3. Blackhole attack:

In blackhole attack, a specific node suddenly stops communicating with the network and thus a blackhole is established. As a result, the received data of the node remains unshared and the other nodes don’t have any idea about the data. The attacker node shares fake routing information in the network so that all packets come to the attacker node. When the packets come to the attacker, attacker denies to forward those packets to the network (Figure: 3).

ISSN: 0971-1260
Vol-22-Issue-16-August-2019

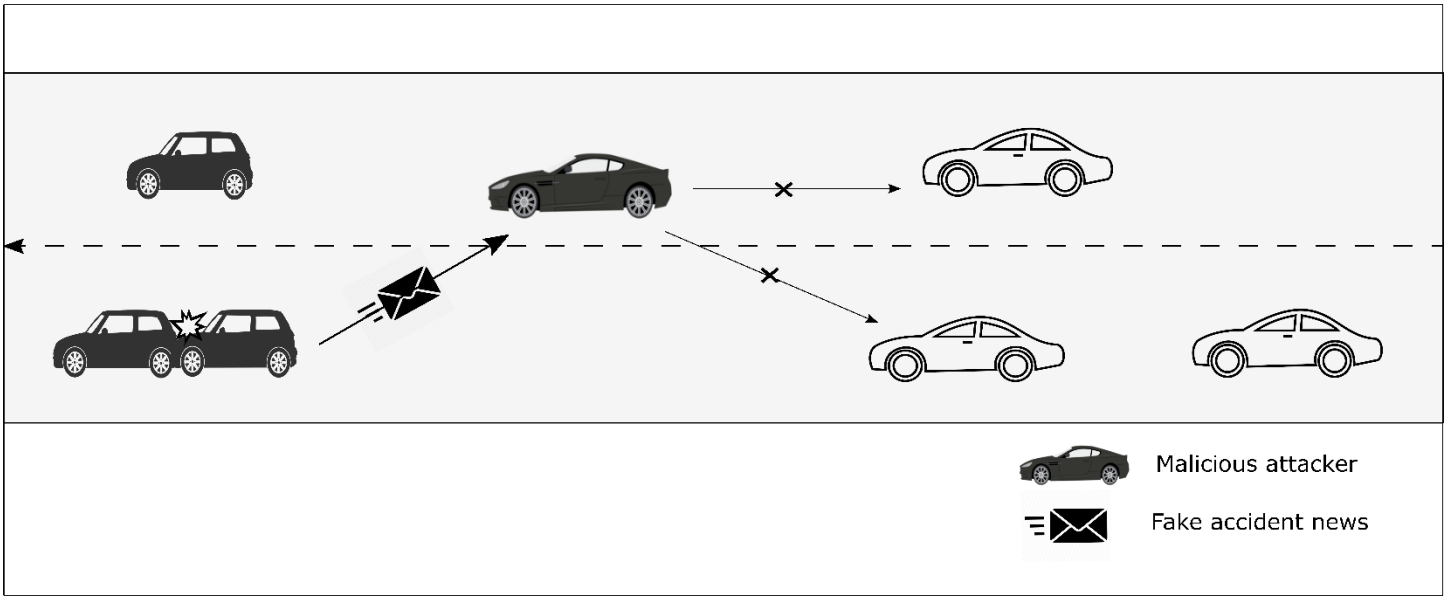

Figure 3: Blackhole attack

4.4. Wormhole attack:

In a wormhole attack, attackers want to modify the network topology to manipulate the traffic [19]. Here attacker node receives the packet and modifying the packet, sends the packet to anothervictim node. Then the packet gets transmitted in the network. As a result, a fake routing path is created and the shortest path shows the best path through the attacker node. When there is only one attacker, the attacker receives a packet at one point of the time and shares the packet after another point to modify the packet. As a result, most of the packets during the point cannot be transmitted properly.

4.5. Fake information attack:

Broadcasting fakeinformation is very crucial problem in VANET. False position information makes the network more inappropriate to use and as a result, drivers get confused about the routs. Attackers inject fake information according to their tastes to change the flow of the traffic. Because of the false position information, many important and emergency information gets lost. Fake information in VANET can occur big accidents or damages.

4.6. Sensor tempering:

OBU of the vehicle is the main component to connect with the RSUs. Attackers try to manipulate the function of the OBU. Attackers attack the nodes for a short time and using short brake, make the application informed that there is a traffic jam on the road. Then the message gets broadcasted in the network. Illusion attack and GPS spoofing are the types of sensor tempering. In an illusion attack, attackers

ISSN: 0971-1260
Vol-22-Issue-16-August-2019

gather traffic information and make new false information. Other drivers receive false information and believe them. Attacker create false information such a way that it seems lots of vehicles on the road and there is a big traffic jam. The attacker also tries to modify the data of own sensors.

In GPS spoofing, attackers inject false information about the GPS location of the vehicle. As a result, the victim node waits for the GPS signal. As the attacker uses a GPS simulator which is more powerful than the main signal, victim nodes easily receive the false signals.

5. SOLUTIONS FOR SECURITY ISSUES:

VANET is introducing an advanced network for vehicular nodes. So, it is very important to maintain the security of the network with the proper model. Many researchers introduced different solutions to provide the best security model for VANET. But a particular model cannot handle all types of attacks. But some model can minimize the effects of the attacks.

As Sybil attack is one of the most dangerous attack in VANET, researchers are trying their best to find out proper solution to detect the attack. To detect a Sybil attack it is needed to detect the corrupted data in the network. The sensor capabilities of all the nodes should be improved. The shared data need to be identified as correct by the nearby authorized nodes. Analyzing the signal strength of the packet the network needs to detect the fake packets. Frequent node authentication can also detect the malicious nodes and can block the Sybil attack.

DoS attacks can bring big damage in VANET. So, a proper solution for this attack is needed. The request detector can get the right request from source to destination. For this, any specific authorized node can be a RSU. Here, the detector gathers information about the source and destination and synchronize the acknowledgment of the transmission. Here, a response detector tries to protect the response packets [20]. To prevent DoS attack a fixed threshold value needs to be set in the network for fixed transmission at a time.

Blackhole attacks can be prevented by the watchdog technique [21]. In this technique, when any node shares a packet to others, then it also checks that the other node is sharing the same packet or not. For this, all nodes need to have a high trust level for sharing the transmission information. Again, using the clustering technique, blackhole attack can be minimized. Here, only the cluster heads are responsible for the main communication.

ISSN: 0971-1260
Vol-22-Issue-16-August-2019

Forwormhole attacks, there are different routing protocols. Those protocols gather information about the proper position of each node through different sensors. The information gets broadcasted in the network. As a result, all the nodes get the exact positions of other nodes.

Fake information-sharing problems can be minimized through message filtering techniques. Here, verified nodes collect data and send it to the RSUs. If any node provides face information to the other nodes, RSUs grab the data and compare with all other data. When RSUs get that the data is appropriate, only then RSUs share the data in the network. A proper verification process can fix the fake position information attack. Multiple RSUs need to verify the nodes at a time so that the attacker node can not share fake position information in the network.

Illusion and GPS spoofing attacks can be prevented by frequent checking of sensors. This process needs to be implemented again and again after a fixed time interval.

6. IDS IN VANET:

IDS is the best solution for VANET security from the very beginning. Different types of IDS provide different types of detection strategies for VANET. But to design VANET with IDS it is mandatory to keep in mind that all IDS cannot cover full security from all types of attacks. So, it is needed to select the type of IDS that can cover most of the portion of security.

6.1. Signature-based IDS:

Signature-based IDS uses previous records and compares them with the gathered new data to find out the malicious events. This IDS uses pattern matching process to get the wrong pattern. Here, the false positive (FP) is low. But, deploying signature-based IDS in VANET is not an easy task. Controller management needs to gather and store the log files of all previous detections to get proper results.

In signature-based IDS cannot detect the new attacks, because there does not have any log about the new attacks. As a result, the new malicious attack can destroy the network.

6.2. Watchdog-based IDS:

In this type of IDS, specific nodes are assigned to monitor other nearby nodes to gather the behavior of those nodes. Here, the source node shares data to the nearby nodes to transfer data to the destination. But when the source sends data to the nearby nodes, it also monitors the activities of the nearby nodes. The source node monitors that the actual data is being sent to the destination properly or not. If there seems any type of disturbance, the source sends an alarm about the incident to the server.

ISSN: 0971-1260
Vol-22-Issue-16-August-2019

6.3. Anomaly-based IDS:

Anomaly-based IDS detects attacks according to the behaviors of the nodes. This IDS makes different profiles of different nodes and updates the details frequently. When it sees any unwanted behavior in the network, it blocks the connection with that particular nodes. Different statistical methods are used to update the profiles. This IDS also use the concept of clustering to update the profiles easily. This process can detect malicious nodes and the detection rate can vary. But this IDS provides high FP rate. This IDS provides high delay and overhead and it takes high computational cost.

6.4. Cross layer-based IDS:

Normally, IDS is deployed in the application layer and it only detects the attacks of just the application layer. But the attacker can target other layers also. In cross-layer IDS, IDS is deployed in different layers. It uses different security detection methods to detect any security fail in the layers. This IDS also use watchdog IDS to improve detection accuracy. This type of IDS provides more delay and overhead.

6.5. Hybrid IDS:

Hybrid IDS is the combination of signature and anomaly-based IDS. This type of IDS uses previous logs and frequently updates the profiles. According to the profile details, this IDS detects the malicious nodes. This IDS can detect both known and unknown attacks in the network. This type of IDS is not cost-effective, because it is not easy to combine multiple IDS and it takes high cost. Though the detection rate is high in this IDS, it takes a long time to detect the attacks.

6.6. Honeypot-based IDS:

Honeypot-based IDS is used to detect selfish nodes [22]. It monitors the traffic and searches for any selfish activity. When it gets any such behavior, it blocks the connection with those particular nodes. This process improves the ratio of packet delivery and decreases end-to-end delay. But this process provides extra overhead and this IDS needs an extra module to improve detection accuracy.

ISSN: 0971-1260
Vol-22-Issue-16-August-2019

Table 1 is showing the comparison of different types of IDS in VANET.

IDS types	Security attacks	Features	Limitations
Signature-based	DoS, False alert, fake congestion	This IDS verifies the identities of all nodes and monitoring the behaviors of the nodes, detects the malicious nodes. Fake messages can be easily detected by this IDS.	• Cannot detect zero-day attacks. • New types of attacks cannot be detected easily. • Depends on the previous records.
Watchdog based	Blackhole, false alert	It uses different statistical methods to detect the greedy nodes that provide false alerts. It provides a threshold to detect attacks. This IDS has low FP rate.	• It detects only specific attacks like selfish, greedy and misbehaving nodes [1]. • Provides extra delay and overhead in the network.
Anomaly-based	DoS, false information, packet drop	This IDS detects the nodes which share false information in the network through different statistical methods. This IDS uses a lightweight clustering technique to detect malicious nodes.	• High delay and overhead. • Cannot detect the types of attacks. • Does not work while updating any profile. • High FP rate. • Not cost-effective.
Cross-layer based	Blackhole	It uses different methods to compare normal and abnormal behaviors.	• Not energy efficient. • Provide extra delay and overhead.
Hybrid	DoS, Blackhole, Sybil, wormhole	It can detect both known and unknown attacks by minimizing the detection errors. It uses both anomaly and signature-based IDS to detect attacks.	• Not cost-effective. • High detection time.
Honeypot based	DoS, Blackhole	It can easily detect the known attacks and also zero-day attack using generalized framework.	• Needs extra modules to improve the detection rate. • High overhead.

Table 1: Comparison of different IDS in VANET

ISSN: 0971-1260
Vol-22-Issue-16-August-2019

7. CONCLUSION:

VANET is now a promising technology in the wireless environment. Users want a lot of safety and security on the road as many people end up there because of other people's abuse and maliciousness. In the future, overcoming these issues requires more effort to achieve a secure VANET environment. This paper presented in a comprehensive way a general overview of most VANET security challenges and their causes and solutions. Here, we provide details of different attacks of VANET. We explain different IDS in VANET to compare the solution for different attacks. Different security challenges and their solutions are also addressed in this paper.Attack or any detection of fake information in VANET is a difficult and challenging issue.With different proper protocols and adaptive detection techniques, computer-based intelligence designs are promising areas that could be explored in future studies to make VANET safer.

REFERENCES:

[1] S. Sharma and A. Kaul, "A survey on Intrusion Detection Systems and Honeypot based proactive security mechanisms in VANETs and VANET Cloud," *Vehicular Communications*, vol. 12, pp. 138–164, 2018.

[2] C. R. Dow, M. H. Ho, Y. H. Lee, and S. F. Hwang, "Design and Implementation of a DSRC Based Vehicular Warning and Notification System," *2011 IEEE International Conference on High Performance Computing and Communications*, pp. 960–965, 2011.

[3] F. Bai and H. Krishnan, "Reliability Analysis of DSRC Wireless Communication for Vehicle Safety Applications," *2006 IEEE Intelligent Transportation Systems Conference*, pp. 355–362, 2006.

[4] K. Indira and E. C. Joy, "Energy Efficient IDS for Cluster-Based VANETS," *Asian Journal of Information Technology*, *14*(1), 37-41, 2015.

[5] G. Loukas, T. Vuong, R. Heartfield, G. Sakellari, Y. Yoon, & D. Gan, "Cloud-based cyber-physical intrusion detection for vehicles using deep learning," *Ieee Access*, *6*, 3491-3508, 2017.

[6] K. A. Alheeti, A. Gruebler, and K. Mcdonald-Maier, "Intelligent Intrusion Detection of Grey Hole and Rushing Attacks in Self-Driving Vehicular Networks," *Computers*, vol. 5, no. 3, p. 16, 2016.

[7] O. Y. Al-Jarrah, C. Maple, M. Dianati, D. Oxtoby, and A. Mouzakitis, "Intrusion Detection Systems for Intra-Vehicle Networks: A Review," *IEEE Access*, vol. 7, pp. 21266–21289, 2019.

[8] O. Y. Al-Jarrah, C. Maple, M. Dianati, D. Oxtoby, and A. Mouzakitis, "Intrusion Detection Systems for Intra-Vehicle Networks: A Review," *IEEE Access*, vol. 7, pp. 21266–21289, 2019.

ISSN: 0971-1260
Vol-22-Issue-16-August-2019

[9] K. Zaidi, M. B. Milojevic, V. Rakocevic, A. Nallanathan, and M. Rajarajan, "Host-Based Intrusion Detection for VANETs: A Statistical Approach to Rogue Node Detection," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 8, pp. 6703–6714, 2016.

[10] S. M. Sangve, R. Bhati, and V. N. Gavali, "Intrusion detection system for detecting rogue nodes in vehicular ad-hoc network," *2017 International Conference on Data Management, Analytics and Innovation (ICDMAI)*, pp. 127–131, 2017.

[11] F. Sakiz and S. Sen, "A survey of attacks and detection mechanisms on intelligent transportation systems: VANETs and IoV," *Ad Hoc Networks*, vol. 61, pp. 33–50, 2017.

[12] A. Kapadia, N. Triandopoulos, C. Cornelius, D. Peebles, and D. Kotz, "AnonySense: Opportunistic and Privacy-Preserving Context Collection," *Lecture Notes in Computer Science Pervasive Computing*, pp. 280–297, 2008.

[13] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," *Proceedings of the 6th annual international conference on Mobile computing and networking - MobiCom 00*, pp. 255–265, 2000.

[14] R. V. der Meulen and J. Rivera, "Gartner says by 2020, a quarter billion connected vehicles will enable new in-vehicle services and automated driving capabilities," *Gartner) Retrieved September*, *18*, 2015.

[15] I. A. Sumra, I. Ahmad, H. Hasbullah, and J.-L. B. A. Manan, "Classes of attacks in VANET," *2011 Saudi International Electronics, Communications and Photonics Conference (SIECPC)*, pp. 1–5, 2011.

[16] J. Grover, M. S. Gaur and V. Laxmi, "Sybil Attack in VANETs: Detection and Prevention," In *Security of Self-Organizing Networks,* Auerbach Publications, pp. 287-312, 2016.

[17] I. Aad, J.-P. Hubaux, and E. W. Knightly, "Denial of service resilience in ad hoc networks," *Proceedings of the 10th annual international conference on Mobile computing and networking - MobiCom 04*, pp. 202–215, 2004.

[18] A. S. K. Pathan (Ed.), "Security of self-organizing networks: MANET, WSN, WMN, VANET," CRC press, 2016.

[19] Y. C. Hu, A. Perrig, and D. B. Johnson, "Packet leashes: a defense against wormhole attacks in wireless networks," IEEE INFOCOM 2003. Twenty-second Annual Joint Conference of the IEEE Computer and Communications Societies (IEEE Cat. No.03CH37428), vol. 3, pp. 1976–1986.

ISSN: 0971-1260
Vol-22-Issue-16-August-2019

[20] K. Verma, H. Hasbullah, and A. Kumar, "Prevention of DoS Attacks in VANET," *Wireless Personal Communications*, vol. 73, no. 1, pp. 95–126, Nov. 2013.

[21] J. Hortelano, J. C. Ruiz, and P. Manzoni, "Evaluating the Usefulness of Watchdogs for Intrusion Detection in VANETs," *2010 IEEE International Conference on Communications Workshops*, pp. 1–5, 2010.

[22] P. Patel and R. Jhaveri, "A Honeypot Scheme to Detect Selfish Vehicles in Vehicular Ad-hoc Network," *Lecture Notes in Networks and Systems Computing and Network Sustainability*, pp. 389–401, 2017.