International Journal of Engineering Applied Sciences and Technology, 2020
Vol. 4, Issue 11, ISSN No. 2455-2143, Pages 267-271
Published Online March 2020 in IJEAST (http://www.ijeast.com)

A SURVEY OF SYBIL ATTACK DETECTION IN VANETS

Dr. M. Preetha, Associate professor,
Pavithra.E, Sudharshna.P, Rakshini.S
Department of Computer Science & Engineering,
S.A. Engineering College, Chennai, Tamil Nadu

ABSTRACT - Vehicular unplanned Networks (VANETs) bring many benefits and conveniences to road safety and future transportation systems. Sybil attack is one among the foremost risky threats since it violates the elemental assumption of VANETs-based applications that each one received information are correct and trusted. Sybil attacker can generate multiple fake identities to false messages. In this paper, we proposed to completely unique Sybil attack detection method for supported by Received Signal Strength Indicator (RSSI), time series, Voiceprint, to conduct widely applicable, lightweight and full-distributed detection for VANETs. Voiceprint adopts RSSI statistic time series as vehicular speech and compares the similarity among all received series. Voiceprint doesn't believe any predefined radio propagation model, and conducts independent detection without support of centralized nodes. We improve Voiceprint for allowing to conduct detection vehicle on Service Channel (SCH) to observation time. And, we extend Voiceprint with change-points detection to identify those illegitimate nodes performing power control. Extensive simulations and real-world experiments demonstrate that Voiceprint is an efficient method considering the worth, complexity and performance.

Keywords: Ad-hoc Network, VANET, Voiceprint, Sybil attack, and RSSI.

I. INTRODUCTION

In the recent years the development of technology in cars has considerably increased. Modern cars are equipped with various electronic components called On-Board units(OBUs) which are responsible for communicating with OBU's of other vehicles and with the Road Side Units(RSU's). So, VANET is the special case of MANET where exchange of safety and non-safety messages takes place between Vehicle to Vehicle (V2V) or Vehicle to Infrastructure(V2I). Figure 1 show the architecture. In VANET messages should exchange securely among Vehicles or with the infrastructure and no attacker should be able to delete or modify them. VANET has also security concerns comprises of availability, integrity, confidentially, authentication and non-repudiations. Different types of attacks are possible on VANET but sybil attack introduced in is one the most harmful attacks as it the root cause of other possible attacks.

In sybil attack, an attacker can generate multiple virtual fake identities/node called sybil nodes to impersonate normal nodes in the VANET. Sybil attack is responsible for violating the fundamental assumptions of VANET. In sybil attack, attacker can create virtual fake identities with false location making the illusion of heavy traffic for other nearby vehicles by which forcing the normal nearby vehicles to take different routes and attacker can get the road with less or no traffic. As sybil attack is the root cause of other attacks, it can also bombard vehicles or infrastructure with heavy traffic which results in choking the bandwidth and hence degrading overall performance of the network. Sybil nodes are also responsible for black hole attack in which sybil nodes could drop all the messages go through them in multipath routing. Vehicular Ad-Hoc Network (VANET) is a specific type of Mobile Ad-Hoc Network (MANET) that provides communication between (1) nearby vehicles and (2) vehicles and nearby roadside equipment

The main benefit of VANET communication is enhancement of passenger safety by exchanging warning messages between vehicles.

1. VANETs differ from MANETs in high mobility of nodes, large scale of networks, geographically constrained topology, and frequent network fragmentation. Most of the research on VANET is concentrated on Medium Access Control (MAC) layer and therefore the network layer.

International Journal of Engineering Applied Sciences and Technology, 2020
Vol. 4, Issue 11, ISSN No. 2455-2143, Pages 267-271
Published Online March 2020 in IJEAST (http://www.ijeast.com)

2. VANETS aim to build applications such as collision avoidance, route changing, and so on. Security of vehicular networks remains largely an explored area.

3. VANET, being a wireless network, inherits all the security threats that a wireless system has to deal with. VANET security is critical because poorly designed VANET is vulnerable tonetwork attacks, and this can compromise the safety of drivers.

4. A security system should ensure that transmission comes from a trusted source and is not a tampered en-route by other sources.

5. It should also strike a balance with privacy because implementing security and privacy together in a system is contradictory.

Types of sybil attack
I. In a direct attack, the honest nodes are influenced directly by the sybil node(s).
II. In an indirect attack, the honest node(s) are attacked by a node which communicates directly with the sybil node(s). This middle node is compromised as it's under malicious influence of sybil node(s).

Some of these attacks are briefly explained subsequently.

1. Bogus information: during this case, attackers are insiders, rational, and active. They can send wrong information within the network in order that it can affect the behavior of other drivers. For example, an adversary can inject wrong information a couple of nonexistent traffic jam or an accident diverting vehicles to other routes and freeing a route for itself.

2.Cheating with sensor information: This attack is launched by an attacker who is insider, rational, and active. He uses this attack to alter the perceived position, speed, and direction of other nodes in order to escape liability in case of any mishap.

3. ID disclosure: An attacker is insider, passive, and malicious. It can monitor trajectories of a target vehicle and may use this information for determining the ID of a vehicle.

4. Denial of service (DoS): Attacker is malicious, active, and local in this case. Attacker may want to bring down the network by sending unnecessary messages on the channel. Example of this attack includes channel jamming and injection of dummy messages

5. Replaying and dropping packets: An attacker may drop legitimate packets. For example, an attacker can drop all the alert messages meant for warning vehicles proceeding toward the accident location. Similarly, an attacker can replay the packets then event has been occurred to make the illusion of accident.

6. Hidden vehicle: This type of attack is possible in a scenario where vehicles smartly try to reduce the congestion on the wireless channel. For example, a vehicle has sent a warning message to its neighbors and it is awaiting a response. After receiving a response, the vehicle realizes that its neighbor is during a better position to forward the warning message and stops sending this message to other nodes. This is because it assumes that its neighbor will forward the message to other nodes. If this neighbor node is an attacker, it can be fatal for the system.

7. Worm hole attack: it's challenging to detect and stop this attack. A malicious node can record packets at one location within the network and tunnel them to other location

through a private network shared with malicious nodes. Severity of the attack increases if the malicious node sends only control messages through the tunnel and not data packets.

8. Sybil attack: During this attack, a vehicle forges the identities of multiple vehicles. These identities are often wont to play any sort of attack within the system. These false identities also create an illusion that there are additional vehicles on the road.

Ways to prevent sybil attack:

A. Giving different power to different members – This is on the basis of reputation systems. Members with different power levels are given different reputation levels.

B. Cost to create an identity – To prevent multiple fake identities in the network, we can put a cost for every identity that aims to join the network. A point to notice is that it makes more sense to form it infeasible to work multiple fake identities at an equivalent time instead of creating new identities. Multiple identities can enforce security, anonymity, censorship prevention.

II. SECURITY ISSUES

In VANET scenarios, every vehicle including emergency vehicles will be equipped with communication capabilities. In addition to collision avoidance, BSMs also can be employed by the authorities for purposes like locating a vehicle that's weakened, chasing vehicle of a criminal, etc. Therefore, it makes tampering with location informed

International Journal of Engineering Applied Sciences and Technology, 2020
Vol. 4, Issue 11, ISSN No. 2455-2143, Pages 267-271
Published Online March 2020 in IJEAST (http://www.ijeast.com)

in BSMs very attractive for attackers. They can produce fake locations to cause accidents, mask truth location of a criminal's vehicle during a police chase and disrupt many other VANET safety applications.

III. WIRELESS LOCATION

Wireless localization is one among the techniques which will be wont to detect fake location advertisements. They use the stationary base stations, aka Road Side Units (RSUs) located at the side of the roads all round the map in VANETs, to perform the localization. These RSUs have a good radio range that permits the defense reaction to be ready to monitor tons of vehicles at an equivalent time. They can hear VANET messages and that they are all connected to every other by wired connections through the infrastructure.

Figure 2 comparison of Sybil attack detecting algorithm

Algorithm	Parameters	Directional Antennae	Cost	Result	Summary
Light Weight Sybil Attack Detection Technique	Speed ,RSS	Not Required	Cheap	90% true positive,10% false negative	The nodes entering in greater than the threshold value are detected as Sybil nodes.
Robust Sybil Attack Detection Technique	Time,Location	Required	Costly	80%true Positive,20% false negative	The nodes having exactly the same path or pattern are detected as Sybil nodes.
P²DAP Sybil Attack Detection Technique	Alarm,RSB, DMV	Not Required	Costly	75%true positive ,25% false negative	The nodes having false alarm rate and detect latency are detected as Sybil nodes.
Hybrid Sybil Attack Detection Technique	Speed,Street map	Required	Costly	80%true positive,20% false negative	To increase vehicle speed and number of nodes to detect as Sybil nodes.
Large Scale of Spider-Monkey	Clock offset,Energy consumption	Not Required	Cheap	78%true positive,22% false negative	The nodes are having energy efficiency to detect as Sybil

International Journal of Engineering Applied Sciences and Technology, 2020
Vol. 4, Issue 11, ISSN No. 2455-2143, Pages 267-271
Published Online March 2020 in IJEAST (http://www.ijeast.com)

IV. POSITION VERIFICATION BY PLAUSIBILITY THRESHOLD:

They use several plausibility thresholds which will be calculated and confirmed using already built-in mechanisms of VANET enabled vehicles. These thresholds are the following:

a. Acceptance Range Threshold: This threshold is set by the maximum radio range of the observer vehicle. The vehicle are going to be ready to receive messages successfully only from the vehicles within this radio range. Therefore, if it receives a message directly from a vehicle that's claiming to be further away than this threshold, that vehicle has got to be lying about its position.

b. Mobility Grade Threshold: This threshold is designed to take into account the maximum speed that a vehicle can have at a certain time. The value it's set to depends on the regulation on the present road and therefore the make/model of the vehicle that's advertising its location. When an edge advertisement is received, the observer vehicle will compare it with the last position advertised by this vehicle and determine if its mobility lie under the mobility grade threshold. .

c. Maximum Density Threshold: There can be a maximum number of vehicles that can be located in a certain area. Maximum density threshold considers the dimensions of a particular area and dimensions of the vehicles that are currently claiming to reside there. If the amount of vehicles therein area is larger than this threshold, all the messages from there'll be ignored by every vehicle since it's a robust indication that there are active Sybil nodes therein area.

d. Map-Based Verification: Some fake locations advertised by attackers might be outside any of road on the map. Each vehicle can use its built-in navigation system to detect these implausible locations. Even though attackers will carefully craft their location advertisements most of the time, it's still a useful sign up the defense mechanisms since it still works for few attack scenarios.

The proposed defense reaction is usually run distributed by individual vehicles without collaboration to detect location attacks. However, detection by these plausibility thresholds might sometimes give false negatives or won't be sufficient alone. In that case, vehicles will collaborate to perform the defense. This involves synchronization of neighbor tables and reactive position requests to build a collective knowledge.

V. CONCLUSION

In this paper, we've discussed about defense methods against Sybil attack in VANETs. According to the studies during this area, each method has some advantages and drawbacks for implementing. Resource testing methods aren't sufficient to implement for Sybil attack detection with high accuracy in VANETs. Authentication methods are more reliable and useful for message integrity, authenticity and privacy and there are suitable methods during this category for practical implementation in urban areas. In contrast, position verification methods are lightweight and straightforward for implementation and if they need high accuracy for position verification, we will use them for other security purposes such as position verification by after receiving location information that periodically broadcast by vehicles for position related applications.

VI. REFERENCE

[1] s. Hadim and N. Mohamed (2006), "Middleware: Middleware Challenges and Approaches for Wireless Sensor Networks," IEEE Computer Society, vol. 7, no. 3.

[2] K. Romer, F. Mattern, and E. Zurich,(2004), "The Design Space of Wireless Sensor Networks," IEEE Wireless Communications, vol. II, no. 6, pp. 54--61.

[3] C. Karlof and D. Wagner,(2003), "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures," in Proc. of the 1st IEEE International Workshop on Sensor Network Protocols and Applications.

[4] A. Perrig, R. Szewczyk, V. Wen, D. Culler, and J. Tygar,(2002), "SPINS: Security Protocols for Sensor Networks," Wireless Networks, vol. 8, no. 5, pp. 521-534.

[5] Q. Hu, D. L. Lee, and W. Lee,(1999), "Performance Evaluation of a Wireless Hierarchical Data Dissemination System," in proc. ACM MOBICOM, pp. 163-173.

[6] M. Fowler,(2003), UML Distilled: A Brief Guide to the Standard Object Modeling Language (3rd ed.). Addison-Wesley.

[7] H. Zimmermann,(2000) "OSI Reference M odel-The ISO Model of Architecture for Open Systems Interconnection," IEEE Trans. on Communications, vol. 28, no. 4, pp. 425-432,.

[8] J. Newsome, E. Shi, D. Song, and A. Perrig,(2004), "The Sybil Attack in Sensor Networks: Analysis & Defenses," in IPSN 2004. Third, pp. 259-268.

[9] Y. Wang, G. Attebury, and B. Ramamurthy,(2006), "A Survey of Security Issues in Wireless Sensor Networks," IEEE Communications Surveys & Tutorials, vol. 8, no. 2.

[10] C. L. Schuba, I. V. Krsul, M. g. Kuhn, E. H. Spafford, A. Sundaram, and D. Zamboni,(2000), "Analysis of a Denial of Service Attack on TCP," in Proc. IEEE Symposium on Security and Privacy, pp. 208-223.

[11] T. Aura, P. Nikander, and J. Leiwo, (2000),"DOS-Resistant Authentication with Client Puzzles," in Proc. Security Protocols Workshop, pp. 170- 177.

[12]Dr.M.Preetha,(2018),” Survey on GPS Based Security Measure for Blind People”, International Journal of Innovative Research in Engineering and Management (IJIREM), Vol.5, No 2.

[13] Preetha M & Sugitha S,2016, “A Survey on Misbehavior Report Authentication Scheme of Selfish node Detection Using Collaborative Approach in MANET”, International Journal of Engineering Science and Computing, vol. 6, no. 5, pp. 5381-5384, ISSN 2321-3361