DETECTION AND LOCALIZATION OF IDS SPOOFING ATTACK IN WIRELESS SENSOR NETWORK USING VANET

Meenakshi B[1], Aishwarya K[2], Dhivya S[3]

[1,2]B.E., Computer Science and Department, Jeppiaar SRR Engineering College, Chennai, India
[3]M.E., Assistant Professor of CSE Department, Jeppiaar SRR Engineering College, Chennai, India

---***---

Abstract - *Wireless spoofing attacks are simple to launch, it plays a major role within the performance of wireless device networks. Although the identity of a node are often verified through crypto logic authentication, standard security approaches aren't invariably fascinating due to their ovserhead needs. The difficult tasks in Wireless device Network are identification of spoofing attackers, determination of variety of attackers, localization of multiple adversaries and eliminating them. The bunch approach is employed to notice the spoofing attackers and localize them. This approach fails to predict the attackers accurately. To overcome this drawback, proposes Intrusion Detection System (IDS) to notice the spoofing attackers. The cluster head act, as IDS to observe the behavior of nodes in their cluster like packet transmission that helps to spot the misbehaving nodes in wireless device network. The simulation result clearly shows that the projected theme detects the spoofing attackers in Wireless device Network with efficiency and robustly.*

Key Words: **– Wireless Sensor Network, Intrusion Detection System, Spoofing Attacks, Data Transmission, VANETs**

1. INTRODUCTION

VANET is an emerging technology that targets to incorporate wireless technologies within ITS (Intelligent Transportation System) in order to increase safety and comfort of drivers. It was evolved from MANET (Mobile Ad-hoc Network), but still maintains its uniqueness due to its characteristics like highly mobile vehicle nodes, frequent disconnection of links, highly dynamic topology, frequent make and break of links. A DSRC (Dedicated Short Range Communication) system in 5.9GHz band is formulated by US FCC (Federal Communications Commission) to benefit the safety of life of drivers and passengers. IEEE 802.11p standard is provided by IEEE to standardize WAVE (Wireless Access for Vehicular Environments).

Among these advancements, the idea of conveyance Ad-hoc NETWORKS (VANET) came into limelight that has opened new potentialities to avail the utilization of safety applications. VANET refers to a network created in an ad-hoc manner wherever completely different moving vehicles and alternative connecting devices are available contact over a wireless medium and exchange helpful info to one another. The communication between devices expands in like approach wherever nodes are unengaged to be part of and leave the network. The new vehicles being launched in the market are currently returning with equipped on board sensors that build it simple for the vehicle to simply be part of and merge within the network and leverage the advantages of VANET.

VANET are often characterized by following factors:

• Dynamic topology- The speed and direction of vehicles changes perpetually thereby leading to high dynamic topology

• Intermittent connectivity- property between devices changes terribly oftentimes like affiliation between 2 devices exchanging info will disconnect anytime. The explanation behind frequent disconnection is high dynamic topology.

VANET aims to produce communication between totally different neighboring vehicles. As per the rules of IEEE 1471-2000 [10, 11] and ISO/IEC 42010 [12], the entities in a very VANET is divided into three domains

1) Mobile domain: Mobile domain contains of two elements. First is vehicle domain that encompasses all the vehicles that are moving perpetually like buses, cars, trucks etc. Second half is mobile device domain that contains of all the transportable handy devices like PDAs, laptop, GPS, smart phones etc.

2) Infrastructure domain: It conjointly contains of two elements. Margin infrastructure domain contains of stationary margin entities like traffic lights, poles etc. Whereas, central infrastructure domain encompasses the central managing centre like vehicle management centre, traffic management centre etc.

3) Generic domain: It contains of web infrastructure and personal infrastructure. As an example, different nodes and servers and alternative computing resources operating directly or indirectly for a VANET come beneath generic domain.

In spite of existing 802.11 security techniques as well as Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), or 802.11i (WPA2), such methodology will solely defend information frames—an offender can still spoof management or management frames to cause vital impact on networks.

2. RELATED WORK

In the year of 2010, Isaac .J.T, Caamara .J.S revealed a paper on "Security attacks and solutions for vehicular ad hoc networks". They mentioned a number of the foremost security attacks that are reportable on VANETs before and in 2010. They bestowed additionally the corresponding security solutions that are projected to forestall those security attacks and vulnerabilities. The main security areas that they targeted on embrace namelessness, key management, privacy, reputation, and placement. Namelessness could be a crucial issue in VANETs regarding the physical identity of mobile nodes (i.e., vehicles) that ought to be unbroken secret in unauthorized components' point of read. Key management deals with issues on generating, distributing, and storing keys. For unplanned networks, there are three main approaches for key management reportable by the literature, namely key exchange, key agreement, and key management infrastructure. In VANETs, the defense against compromised nodes, and malicious ones are often assured by applying such forms of systems.

In 2012, within the paper "Survey on Security Attacks in vehicular ad hoc Networks (VANETs)" , Mohammed Saeed Al-kahtani known completely different security attacks, classified them, compared their defending mechanism in VANETs and prompt some future potentialities during this space. The author categorized three varieties of aggressor as follows:

2.1 INSIDER VS. OUTSIDER

If the aggressor may be a member node World Health Organization will communicate with different members of the network, it will be referred to as an insider and ready to attack in varied ways in which. Whereas, an outsider, who is not authenticated to directly communicate with different members of the network, have a restricted capacity to perform an attack (i.e., have less sort of attacks).

2.2 LOCAL VS. EXTENDED

An assaulter is taken into account as native if it's restricted in scope, whether or not it possesses many entities (e.g., vehicles or the base stations). Otherwise, AN extended assaulter broadens its scope by dominant several entities that are scattered across the network. This distinction is particularly vital in wormhole attacks that we are going to describe later.

In 2013, Irshad Ahmed Sumra projected five totally different categories of attacks [2] and each category is expected to supply higher perspectives for the VANETs security (Table 1). This paper tried to propose a classification and an identification of various attacks in VANETs..

3. PROPOSED SYSTEM

VANET maintains its uniqueness due to its special characteristics like frequently changing topology, highly mobile vehicle nodes and frequent make and break of links. Due to these characteristics, evaluation of network performance by monitoring network elements is difficult. Thus, in our approach, we studied network tomography to evaluate the network performance in a dynamic VANET. This technique does not require any cooperation from the network elements to evaluate network performance. In our approach, we infer link delay from estimated end-to-end delay using network tomography.

The use of RSS-based spatial correlation and a physical property associated with each wireless node is hard to detect the corruption and are not relevant on cryptography for detecting spoofing attacks. Attackers who have different locations then the legitimate wireless nodes are concerned, spatial information is used not only to identify the presence of spoofing attacks but also to localize adversaries. Spoofing could be a scenario during which one person or program with success masquerades as another by falsifying knowledge and thereby gaining an illegitimate advantage.

In a large-scale network, multiple adversaries might masquerade because the same identity and collaborate to launch malicious attacks like Network Resource Utilization and DOS (Denial-of-Service) attack quickly. Among various types of attacks, spoofing attacks are easy to launch that degrades the network performance highly. The nodes information in the cluster is collected by cluster head which acts as Intrusion Detection System (IDS) for monitoring the cluster member. If the IDS find the attacker, it passes the alarm message to the source node which eliminates the attacker. The K-Means clustering approach and Intrusion Detection System mechanism are implemented to determine the number of spoofing attacks and localize the same in wireless sensor network.

3.1 NETWORK FORMATION*:*

In this module, create a network formation consisting of nodes. Each node acts as a neighbour and has its own distance and range. Create nodes by giving range and distance as input which in turn describes the vehicle location. Each node has number of channels to reach the destination. Create 'n' number of nodes based on requirement to form network environment or network formation.

Wireless sensor networks (WSN) are composed of a finite set of network sensor devices geographically distributed during a given indoor or outdoor atmosphere (usually predefined). A WSN aims to collect environmental information and therefore the node devices placement could also be best-known or unknown a priori. Network nodes will have actual or logical communication with all devices; such a communication defines a topology consistent with the appliance. As an example, there are often a WSN with each sorts of topologies being the identical (mesh, star, etc.)...

Centralized formation techniques are appropriate for networks during which the process power capability depends totally on a novel device. In such cases, this device is to blame for the process, coordination, and management of the perceived info activities. It additionally forwards this information to a sink node. The most benefits of this approach are as follows:

1. Centralized schemes permit additional economical energy management.
2. Roaming is allowed within the network.
3. Network coverage analysis is easily simplified.
4. Context info available permits a higher application style (placement of nodes, application awareness, etc.).

3.2 TRAFFIC REDUCTION*:*

Traffic accidents became a vital drawback for governments, researchers and vehicle manufacturers over the previous few decades. However, accidents are unfortunate and regularly occur on the road and cause death, injury to infrastructure, and health injuries. Therefore, there's a necessity to develop a protocol to avoid or prevent traffic accidents at the intense level so as to scale back human loss.

In VANETs, the topology of the network keeps dynamical because of the high quality of vehicles; therefore the network is taken into account as AN ad-hoc network. It permits vehicles to sense their setting and exchange their perceived information with surrounding vehicles. AN infrastructure named Road side Units (RSU) is put in on the roads to help the vehicles taking possession its section. Customary IEEE 802.11p has been introduced, significantly for transport communication, that permits ad-hoc communication (the p denotes the particular version for communication between vehicles). There are 3 modes of communication in VANETs: Vehicle to Infrastructure (V2I), Vehicle to Vehicle (V2V), and Vehicle 2 Hybrid (V2X) communication. Vehicles communicate with one another so as to urge a much better understanding of the encompassing atmosphere to forestall any dangerous things. Drivers should be timely warnings regarding any expected dangerous things so as to avoid accidents

Normally the traffic in MATLAB is generated from the traffic agents such as TCP and UDP agents whose parameters are based on the certain statistical distribution. It is to demonstrate how traffic agents in MATLAB simulator are used to generate different types of traffic based on the real traffic network. It consider every traffic routes as alpha, beta, gamma,... and compare every routes in determined range and gives the result of less traffic. In this proposed system, packet loss level is considerably low. Therefore, we can reduce accident in highways and moreover, we can reduce traffic in main areas.

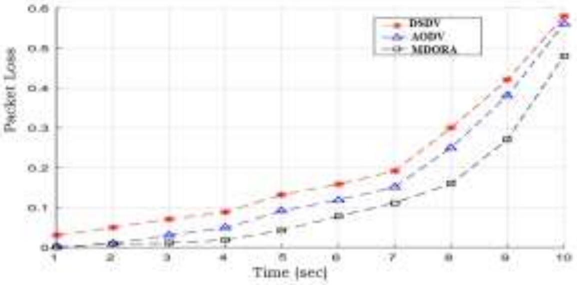

Chart-1: Packet loss during Data Transmission

3.3 INCREASE EFFICENCY USING MDORA ALGORITHM:

MDORA may be a position-based routing protocol designed for VANETs that generates on-demand routes between vehicles. During this algorithmic program, time period traffic knowledge is employed to create an ad hoc region property graph between the supply vehicle and its neighboring vehicles. The ad hoc region property graph determines the space between neighboring vehicles. Looking on the longest period of communication lifespan, intra-vehicular distance, and destination vehicles' position knowledge, an acceptable path is chosen for knowledge routing.

In these modules, we tend to increase efficiency than the existing system .where the information will solely transfer to the nodes once they travel in same speed when one node travel additional quick or slow, the datum cannot transfer to different nodes. To over come back this drawback we tend to use MDORA algorithmic rule that is additional efficient than the AODV (Ad hoc On-Demand Distance Vector) and DSDV (Distance supply Distance Vector) wherever data can be transfer to nodes at any speed by victimization the algorithm we will additionally increase the speed passing the information more efficient and also more firmly in order that data can be pass to nodes without any method of dropping the datum.

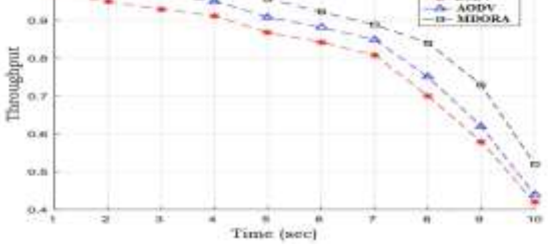

Chart-2: Throughput calculation during peak time using MDORA

3.4 FINDING SHORTEST DISTANCE USING HYBRID ROUTING PROTOCOL*:*

At the heart of any routing protocol is that the algorithmic rule (the "routing algorithm") that determines the trail for the packets purpose of a routing algorithmic rule is straightforward : given a group of routers ,with links connecting the routers, a routing algorithmic rule finds a "good" path from source to destination Hybrid routing protocol (HRP) could be a network routing protocol that combines the features of DVRP and LSRP. The procedure of considering distance factor (Dist f) to find the following hop neighbor vehicle is given in Fig. 5. Line section SD connexion the source and therefore the destination is drawn to project vehicles n 1 and n 2. The shortest distance between the source and the destination vehicles is denoted by dc whereas d and d′ denote the distance from intermediate vehicles (n 1 and n 2) to the source and therefore the destination, severally. Dn 1 and Dn 2 are the distances that live the progress of vehicles n 1 and n 2 from the source vehicle toward the destination vehicle, and this distance will be calculated from the formula below, that is outlined as follows:

$$\mathrm{Distf}=\frac{\mathrm{Dist}_2(S,D)+\mathrm{Dist}_2(S,n)-\mathrm{Dist}_2(n,D)}{2\times \mathrm{Dist}_2(S,D)}$$

$$\mathrm{Dist}\ (S,D)=\sqrt{(xDx - xSx)2 + (yDy - ySy)2}$$

$$\mathrm{Dist}\ (S,n)=\sqrt{(xnx - xSx)2 + (yny - ySy)2}$$

$$\mathrm{Dist}\ (n,D)=\sqrt{(xDx - xnx)2 + (yDy - yny)2}$$

Hence, the vehicle with the maximum distance (Dist f) toward the destination are chosen because the next hop. Below fig shows that consistent with the gap issue choice, vehicle n 2 ought to be most well-liked to vehicle n 1.

The communication lifetime factor (CLT f) defines the period that a vehicle remains within the radio range of the forwarder. Thus, whereas choosing the following hop, supported the communication lifetime factor, a vehicle predicts the communication link duration time with its neighbors. It's assumed that 2 vehicles, i and j, are among every other's transmission range denoted by r, coordinates (x i, y i) and (x j, y j). Also, let v i and v j be the velocities of vehicles i and j, severally. CLT f between 2 vehicles is going to be computed as follows:

$$\mathrm{CLTf}=\frac{-(ab+ac)+\sqrt{(a)^2r^2-(ac-ab)^2}}{a^2}$$

where $a = v_i - v_j$, $b = x_i - x_j$, and $c = y_i - y_j$

Note that when $v_i = v_j$, the communication lifetime CLT_f becomes infinity. After computing Dist f and CLT f factors for every neighbor vehicle, the supply vehicle initiates a neighbor table (Neighbor_table) comprises of Neig_ID, Dist f , and CLT f . Then, the supply vehicle types the Neighbor_table per the Dist f factor, that is that the highest Dist f.

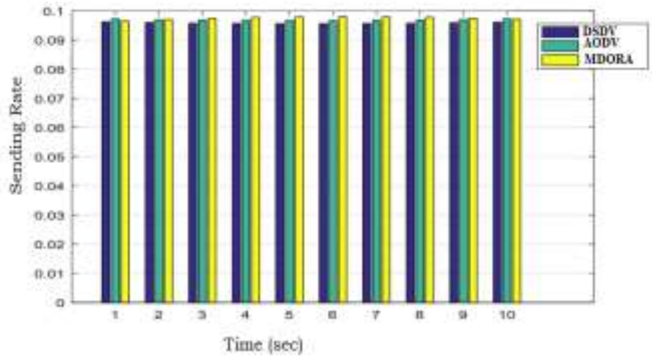

Chart-3: Data sending rate using MDORA

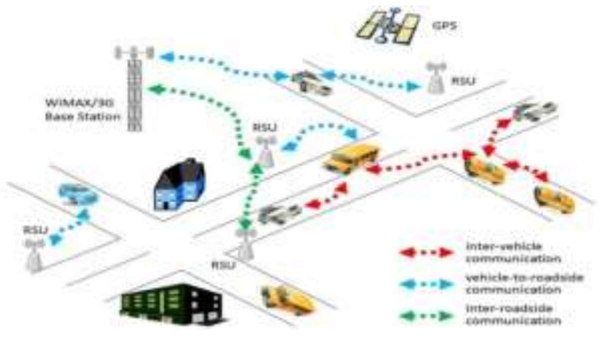
GPS
RSU
WIMAX/3G Base Station
RSU
RSU
RSU
inter-vehicle communication
vehicle-to-roadside communication
inter-roadside communication

Fig-1: Architecture diagram

4. RESULT AND DISCUSSION

This project projected to use received signal strength-based abstraction correlation, a physical property related to every wireless device that's exhausting to falsify and not dependent on cryptography because the basis for detection spoofing attacks in wireless networks. The approaches will each detects the presence of attacks as well as confirm the quantity of adversaries, spoofing the identical node identity, in order that will localize any variety of attackers and eliminate them.

In this paper, the projected MDORA provides an opti-mal route for end-to-end information delivery in urban VANET environments. MDORA consists of 2 phases, ad hoc discovery section and route establishment and data transmission phase. The projected routing mechanism is based on hop by hop, that minimizes management overhead by shrewd the route with the smallest amount variety of possible hops over a supreme distance. Simulations are performed at different hours throughout the day. The simulated results have shown that MDORA proves to be superior than the AODV in terms of throughput, packet delivery ratio and communication overhead.

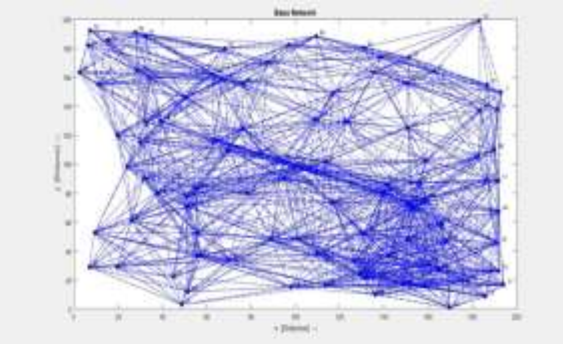

Fig-2: Data transfer using MDORA Algorithm

5. CONCLUSIONS

The primary purpose of this thesis is to design an economical routing algorithmic rule in VANET surroundings to enhance the performance of existing position based mostly routing approaches in VANETs. The frequent network disconnections caused by high speed quality of vehicles is known as a significant issue. It decreases packet delivery rate, will increase packet delay and increases routing overhead in VANET surroundings. Accident zone are reduced in VANET surroundings. The time delay reduction can produce a lot of faster reply in VANET surroundings.

Spoofing attack is one among the most important problems in wireless sensor network. The identification of spoofers and localization of the identical may be a difficult task in wireless sensor network. During this paper, numerous algorithms are projected. Spoofing attack detection and localization in wireless sensor network are extensively studied. Further, this paper can facilitate the research worker to create novel methodology in order to spot the spoofing attack similarly as remove or disable the identical in wireless sensor network effectively with less value.

6. REFERENCES

1. E. Elnahrawy, X. Li, and R.P. Martin, “The Limits of Localization Using Signal Strength: A Comparative Study,” Proc. IEEE Int’ Conf. Sensor and Ad Hoc Comm. and Networks (SECON), Oct. 2004.
2. P. Bahl and V.N. Padmanabhan, “RADAR: An in-Building RFBased User Location and Tracking System,” Proc. IEEE INFOCOM, 2000.
3. P. Enge and P. Misra, Global Positioning System: Signals, Measurements and Performance. Ganga-Jamuna Press, 2001.989Jie Yang, Yingying (Jennifer) Chen, Senior Member, IEEE, Wade Trappe and Jerry Cheng. (2013). Detection and Localization of Multiple Spoofing Attackers in Wireless Networks. IEEE. 24 (1), p44-58
4. Akyildiz I., Su W., Sankarasubramaniam Y., Cayirci E. A survey on sensor networks. IEEE Commun. Mag. 2002; 40 : 102–114.
5. Tubaishat M., Madria S. Sensor networks: an overview. IEEE Potentials. 2003;22 : 20–30.