INTERNATIONAL JOURNAL OF TECHNOLOGY AND COMPUTING (IJTC)
ISSN-2455-099X,
Volume 2, Issue 5 May 2016.

A CO-OPERATIVE VARIOUS ATTACKS DETECT FOR LOCATION BASED APPLICATION IN SECURE NETWORK

RamSharanjit Singh [a], Varun Sandhuja [b]
[a] *M.Tech Student ECE, Khehrahappy35@gmail.com*
[b] Assistant *Professor, ECE, Department, varun.cgctc@gmail.com*
[a,b] *Department of ECE, CGC (T.C), Punjab, India*

ABSTRACT

Sybil attack is one of the vital/ serious attacks to vehicular ad-hoc network, because it numerous damages the security of vehicular ad-hoc network and even leads to a warning to lives of teamsters and passengers. Vehicle location is one of the major valuable pieces of information in VANETs. In this paper, we studied a solution to detect the malicious attack based on differences between the normal motion attackers of vehicles and abnormal ones. Each node can accomplish the attack detection self-sufficiently with the limited assistance from the structures of VANETs. An Improve the probability of planned with limited environments at the early deployment stages of VANETs. The independency and feasibility of algorithm are more robust than the previous solutions that rely on addition of neighbouring node.

Keywords: Sybil attack, Vehicular ad-hoc network, Motion Attackers, feasibility.

I. INTRODUCTION

Latest technologies offer modern vehicles not only new flowing design but also new devices. An introduction of novel vehicle devices, modern vehicles [1] are more intelligent and secure. The provision of on-board GPS – Global Positioning System devices has revolutionized driving. Correspondingly, the new introduction of short range radar on few top of the line models promises to minimize the numerous offender- sprees and other accidents. Vehicle cameras are famous these days to invent images of surrounding vehicles. Using image processing technology, motorists can be supported by these cameras. Other new devices, such as magnified sensors, are used in intelligence vehicle.
VANETs is a vital component of intelligent transportation systems and used for communication and co-operative driving between cars on the road. VANETs have particular features like;

1) Distributed Processing and
2) Organized Networking a great several nodes.

In distribution and the speed of these sensors/ vehicles, a constrained but extremely variable network topology, Communication conditions and mobility patterns, Data transmissions blocked by buildings, Recurrent partition due to the high mobility and lastly there are no important power constraints. Vehicle can exchange alternative, traffic events, weather circumstances, road data among other input (Vehicles) [2] and RSUs i.e. Road Side Units, as well as transferring advertisements. Vehicles are capable of forming ad-hoc networks with no prior knowledge of each other, whose secure level is very less and can be attacked easily. Secure network has always been a matter in vehicle ad-hoc networks which must be seriously considered and a secure infrastructure has to be designed and developed.

IJTC.ORG

We focus on Sybil attack where an attacker assumes multiple id while a basic contributor is allowable only one identity by making a large numerous of duplicate is allowable or by stealing from real sensors/nodes in the network. The characteristics of these networks such as: Communal wireless medium, the extremely dynamic network topology nonappearance of conventional security infrastructures pose a numerous of non-trivial challenges to secure design. Susceptibilities of ad-hoc networks are not incomplete unfortunately in the issue of shared wireless medium but also in routing instrument and auto configuration used. These mechanisms are based on faith between participating nodes. If a node has mischievous behaviour, all facilities offered by the co-operative network will be paralyzed. An effective way to individuality when an attack occurs in a VANET is developed of an Intrusion Detection System.

The level of security is defines in terms of necessities, such as confidentiality, assertion of information is ethical and difficult; it is conscientious access to the information by authorized people, cleanness and non-repudiation. Subsequently from some threats a Sybil attacks, in which a malicious vehicle create an impression of traffic holdup by creating numerous individualities. Therefore, Sybil attacks are planned very deliberate security threat to ad-hoc and sensor networks, there are three types of lines against Sybil attacks namely;

1. Radio resource testing
2. Registration and
3. Position Verification.

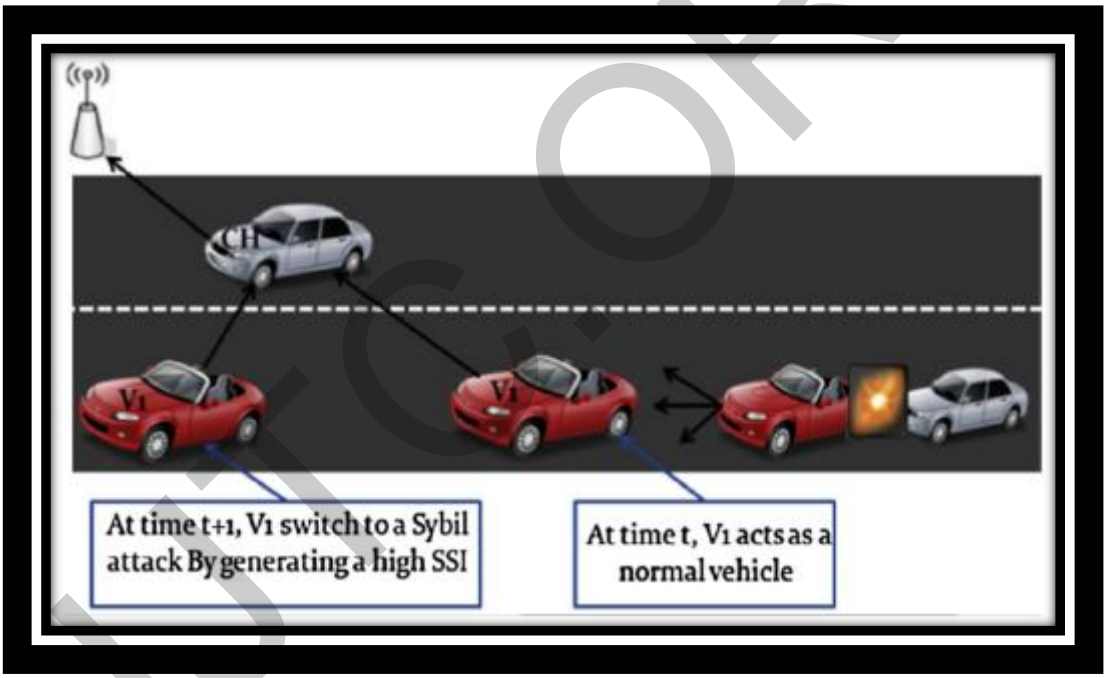

Fig. 1: Attack Scenario: Sybil Attack

Sybil Attacks might be damaging to a variation of vehicle ad-hoc network applications. For Example, a greedy driver can formulate that a several of vehicles [3] are travelling nearby, which creates a deception of traffic congestion. Then, other vehicles will select threats.

II. Intrusion Detection System

In normal terms "Intrusion" is defined as 'any set of movements that attempt to compromise integrity, privacy or accessibility of resource' such as protocols and systems which are meant to offer services in VANET and can be a target of attacks such as DDos Attack. Intrusion detection can be used as a second line of defence to protect network systems since once an intrusion is detected response can be put in place reduce the[4] damage or presentation counter offensives. Intrusion detection assumes that 'network events are observable', which means that packets/bits that go through the network hardware interface are arrested

and examined. The apprehended data is called audit data on the basis of this audit data defining whether it is a significant deviation from normal system performance, if yes the IDS infer that the system is under attack.

A. Attacks in VANET

VANET there are some problems high mobility, real time guarantee, Privacy and Authentication, location awareness, Delay in VANET is fronting many attacks. Some of them are described as follows:

1) DDOS Attacks: DDos attacks are a type of attack which is caused by the network insiders and outsiders offer the network which is not available to [5] the real users. This is done by overflowing the control channel with high amount of naturally generated communication and stopping the connection.

2) Sybil Attack: Such Attacks are forging the individuality of many vehicles which are used to cast any type of attack on the system and it is used to decay the connections of network, topologies, network transmission spending.

3) Message Suppression Attack: Kind of attack, attacker discriminative drops the message packets. For the receiver critical information might be hold by these packets.

4) Malicious Vehicle: Confidentially is the most important security obligation of VANETs. To escape being tracked, the use of randomly changing identities is suggested. This can lead to a situation where a malicious vehicle N can easily change its identity to Node S without being punished.

III. Prior Work

Gongjun Yan et al., 2011, suggest a normal active discovery architecture including two components:

1) Eye devices and
2) Ear-devices.

Eye-devices include radar, infrared, camera etc. Ear-device is the wireless transceiver. We achieve local security by recruiting the help of several on-board eye devices to detect contiguous vehicles and to confirm their broadcast position coordinates heard by ear-device. They apply cosine similarity to these data to reach an agreed-location. Solution is established on the widely accepted assumption that the vast majorities of vehicles are honest and behave quickly.

Parastoo Kafil et al.,2012, deliberate and motivate the needs for real traffic simulation with standard network reproduction and explain the attack models for an individual Sybil attacker .They consider that the attack model can be altered in each traffic scenario and cultured movement path such as urban traffic model having a potentially high influence related to uniform highway traffic model. Also they simulate and compare attacker models in two positions:

1) Near the source and
2) Near the destination of data packet sending.

Mohammed ERRITALI et al.,2013, In wired networks the attacker wants to gain access to the physical media to make an attack. In wireless networks the situation is much different, there are no firewalls and gateways in residence hence attacks can take place from any location within radio coverage area. All mobile nodes in ad-hoc network is an autonomous unit in itself free to move independently. This means a node with not satisfactory physical protection is very much susceptible to be compromised. It was difficult to track down a single co-operated node in a large network, attacks stemming from a compromised node were far more damaging and much harder to detect. Attack countermeasures such as digital signature and encryption, can be used as the chief line of defences for plummeting the promises of attacks. However, these systems had limited prevention in general, and they were designed for a set of known attacks. They were unlikely to avoid most current attacks that were designed to sidestep existing security measures.

Usha Devi Gandhi, et al., 2014 in these network vehicles can joininto one another so that a mobile internet was created. It was used for Intelligence Traffic System. Very well-known automotive companies like BMW and Ford encourages this term. In VANET the mobile nodes were well prepared with On board Radio

IJTC.ORG

Transponder that was useful in communication with other nodes in a network. In order to found communication among the vehicles VANET originates with communication points by road substructure.

Mahdiyeh Alimohammadi et al., 2015 suggest a secure protocol for solving two conflicting goals privacy and Sybil attack in vehicle to vehicle communications in VANET. The planned protocol was based on the Boneh Shacham short group signature scheme and batch verification. Experimental consequences demonstrate efficiency and applicability of the suggested protocol for providing the necessities of privacy and Sybil attack detection in V2V communications in VANET [10].

IV. Proposed Work

Our Proposed work Firstly, Initialize the vehicular ad-hoc network, to create the network focus in data transmission. Sensors are plotting in a particular network to transfer the data one node to another node. To find the source and destination for vehicular ad-hoc network. To generate the coverage set for calculate the distance in particular range. To use the routing protocol for detection. Information Transfer one node to another node attacker will come and loss the information in particular node. Apply optimization technique

for prevention and to save the information in particular nodes. Optimization Technique always gives the reduce index and using the fitness function for generates the fit value. To evaluate the performance parameters like throughput, bit error rate etc. Compare the result in previous parameter.

IJTC.ORG

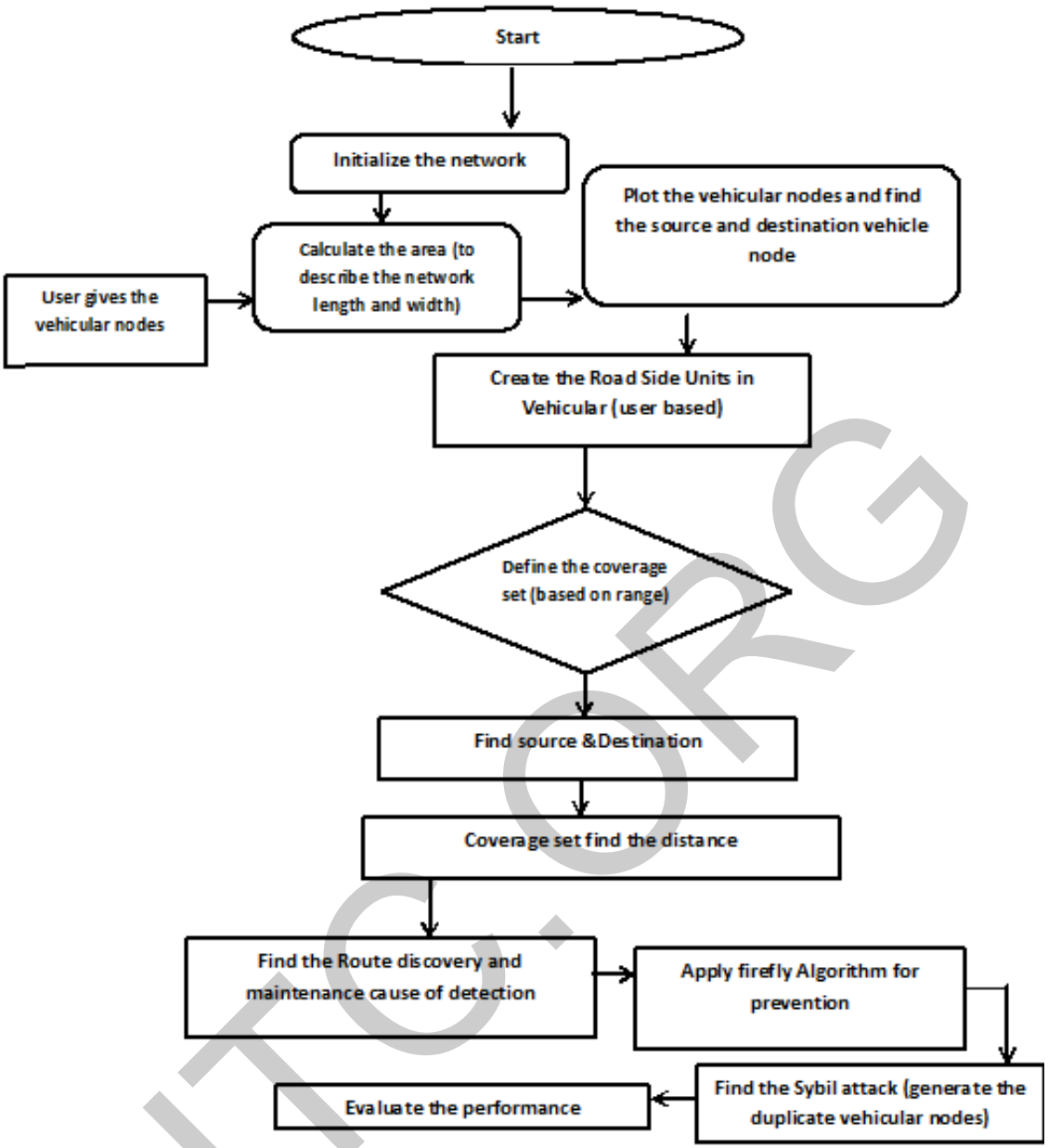

Figure no: 2 Proposed Work

IJTC.ORG

V. CONCLUSION

In VANET, numerous attacks are being activated by the malicious nodes. Therefore keeping in view above experiments there is a need to advance the efficiency of Vehicle protocol so that it may be able to controller both, the features which make wireless communication unreliable and also provision the above application encounters to a large extent. All the difficulties discussed in this paper can be higher if some of the incorrect information can be flooding in the network. The incorrect information can be flooding in the network by malicious vehicles. These malicious vehicles can damage the network performance by generating some security attack.

REFERENCES

[1] Quyoom, Abdul, et al. "A novel mechanism of detection of denial of service attack (DoS) in VANET using Malicious and Irrelevant Packet Detection Algorithm (MIPDA)." *Computing, Communication & Automation (ICCCA), 2015 International Conference on*.IEEE, 2015.
[2] Gantsou, Dhavy. "On the use of security analytics for attack detection in vehicular ad hoc networks." *Cyber Security of Smart Cities, Industrial Control System and Communications (SSIC), 2015 International Conference on*. IEEE, 2015.
[3] Saggi, MandeepKaur, and RanjeetKaur. "Isolation of Sybil attack in VANET using neighboring information." *Advance Computing Conference (IACC), 2015 IEEE International*.IEEE, 2015.
[4] KaurP, Harsimrat, and PreetiBansalP. "Efficient Detection & Prevention of Sybil Attack in VANET." (2015).
[5] Grover, Jyoti, Manoj Singh Gaur, and Vijay Laxmi. "Multivariate verification for sybil attack detection in VANET." *Open Computer Science* 5.1 (2015).
[6] Yan, Gongjun, et al. "General active position detectors protect VANET security." *Broadband and Wireless Computing, Communication and Applications (BWCCA), 2011 International Conference on*. IEEE, 2011.
[7] Kafil, Parastoo, MahmoodFathy, and Mina ZolfyLighvan. "Modeling Sybil attacker behavior in VANETs." *Information Security and Cryptology (ISCISC), 2012 9th International ISC Conference on*.IEEE, 2012.
[8] Erritali, Mohammed, and Bouabid El Ouahidi. "A review and classification of various VANET Intrusion Detection Systems." *Security Days (JNS3), 2013 National*.IEEE, 2013.
[9] Gandhi, Usha Devi, and R. V. S. M. Keerthana. "Request Response Detection Algorithm for detecting DoS attack in VANET." *Optimization, Reliabilty, and Information Technology (ICROIT), 2014 International Conference on*.IEEE, 2014.
[10] Alimohammadi, Mahdiyeh, and Ali A. Pouyan. "Sybil attack detection using a low cost short group signature in VANET." *Information Security and Cryptology (ISCISC), 2015 12th International Iranian Society of Cryptology Conference on*.IEEE, 2015.

IJTC.ORG