IJCSE International Journal of Computer Sciences and Engineering Open Access

Research Paper Vol.-7, Issue-7, July 2019 E-ISSN: 2347-2693

The Data Dissemination Resistant Trust Management Scheme for Securing Vehicular Ad Hoc Networks

K. Premkumar[1*] R. Baskaran[2]

[1]Department of Computer Science & Engineering, Manonmaniam Sundaranar University, Tirunelveli
[2]Department of Computer Science & Engineering, Anna University, Chennai, India

Corresponding Author: premkvpt@gmail.com, Tel.: 9842127679

DOI: https://doi.org/10.26438/ijcse/v7i7.713 | Available online at: www.ijcseonline.org

Accepted: 13/Jul/2019, Published: 31/Jul/2019

Abstract— To increased safety and efficiency of road transportation system have promoted automobile manufacturers to integrate wireless communications and networking into vehicles. VANETs have the potential to transform the way people travel through the creation of a safe, interoperable wireless communications network that includes cars, buses, traffic signals, cell phones, and other devices. Due to increasing reliance on communication, computing, and control technologies have become vulnerable to security threats in VANET. To provide the security in VANET by developing the new mechanism which is integrity(data trust), confidentiality, non-repudiation, access control, real-time operational constraints/demands, availability, and data dissemination technique. In our proposed system propose the novel scheme which is called as trust management scheme data dissemination in order to eavesdroppers with threshold based malicious node detection algorithm (TMD) for VANETs that is able to accurately detect and cope with malicious attacks and also evaluate the trustworthiness of both data and mobile nodes in VANETs. At first the data trust is evaluated based on the data sensed and collected from multiple vehicles; after that we evaluate the node trust in two dimensions, i.e., functional trust and recommendation trust. The functional trust is indicating how likely a node can fulfill its functionality. The recommendation trust is indicating how trustworthy the recommendations from a node for other nodes will be, respectively. Finally our experimental result shows our proposed trust management theme is applicable to a wide range of VANET applications to improve traffic safety, mobility, and environmental protection with enhanced trustworthiness.

Keywords— Vehicular Ad-hoc Networks, Wireless Sensor Networks, Time Division Multiple Access.

I. Introduction

VANET(Vehicular Ad-hoc Networks) can be defined as the vehicle to vehicle and vehicle to roadside wireless communication. It provides an important role in high level of safety and convenience to drivers on the road. In other words VANETS may be defined as the technology that uses the moving cars as nodes to create a network. VANET turns each and every participating car into a wireless router or node, allowing cars approximately at a distance of 100 to 300 meters from each other to connect and create a network with a wide range. In that network each node is equipped with wireless communication technology and uses RSU as an access point used together with the vehicles that allows information dissemination in the roads. On-Board Unit (OBU) in the VANET for highways and realizes the vehicle-to-vehicle (V2V) communication. The main application of the VANET is to provide high road safety. Examples may include the Car-2-Car Communication Consortium, the Vehicle Safety Communications Consortium, and Honda's Advanced Safety Vehicle Program, among others. The impulsion of VANET is that in the not-so-distant future vehicles equipped with computing, communication and sensing capabilities will be organized into a ubiquitous and pervasive network that can provide numerous services to travellers, ranging from improved driving safety and comfort, to delivering multimedia content on demand, and to other similar value-added service. Indeed, the fact of being that are networked together promotes car-to-car communications, even between cars that are tens of miles apart. Imagine, for example, a car travels down an interstate and whose passengers are interested in viewing a particular movie. The various blocks of this movie happen to be available at various other cars on interstate, often miles away. The task of collecting blocks of the movie translates, at the network layer, into finding appropriate routes between the various sources cars that are willing to share movie blocks and the receiving car.

APPLICATIONS:

- Safety alerts
- Drivers are alarmed of different road conditions
- Communication between car and road side can be performed by VANET
- Military or police exercise.
- Disaster relief operation.
- Mine site operation.
- Urgent Business meetings

II. Related Work

A. Introduction

We have researched on the topic VANET and listed some of the related work below:

(N.Karthik, V.S.Ananthanarayana,December 2017) The performance of the novel hybrid MAC protocol in terms of energy and delay with offered traffic load has been explored for cluster based wireless sensor network. From simulation results it is evident that for intra-cluster communication, BMA protocol performs the best and achieves 25% reduction in the energy consumption compared to TDMA and 5% reduction in energy consumption than E-TDMA scheme and provides 15% less packet transmission delay by incorporating the proper dynamic scheduling schemes. NanoMAC protocol provides better performance for inter-cluster communication and its energy expended for data transmission is almost 40% less than np-CSMA protocol. The delay of NanoMAC protocol is considerably reduced by 15% without any degradation in the throughput when compared with np-CSMA scheme. This reduction in energy consumption and delay of hybrid MAC protocol can significantly prolong the lifetime of the sensor network. The scarcity of prime (frequencies below 2 or 3 GHz) spectrum is a decades-old problem in wireless communication, and will be for the indefinite future. Recognizing that a static allocation of spectrum over time and space is highly suboptimal.

(Salman Goli-Bidgoli, NaserMovahhedinia
November 2017) The geographic routing in the duty- cycled mobile WSNs and the geographic-distance- based connected-k neighborhood (GCKN) sleep scheduling algorithms for geographic routing schemes to be applied into duty-cycled mobile WSNs. The first geographic-distance based on the connected-k neighbourhood for the first path (GCKNF) sleep scheduling algorithm minimizes the length of the first transmission path explored by geographic routing in duty-cycled mobile WSNs. The second geographic-distance based connected- k neighbourhood for the entire paths (GCKNA) sleep scheduling algorithm reduces the length of all paths searched by geo- graphic routing in duty-cycled mobile WSNs. The performance evaluations by the simulations, shows that when there are mobile sensors, geographic routing can achieve much shorter average length for the first transmission paths searched in mobile WSNs employing GCKNF sleep scheduling and all transmission paths explored in mobile WSNs employing GCKNA sleep scheduling compared with those in mobile WSNs employing CKN or GSS sleep scheduling. Geographic routing, a promising routing scheme in the wireless sensor networks (WSNs), shifting towards duty-cycled WSNs in which Mobile sensors are sleep scheduled to reduce the energy consumption.

(MaBora Karaoglu Wendi Heinzelman May2015) The multipath load balancing technique for congestion control (MLBCC) in MANET to efficiently balance the traffic load. Here, the selection of source node is done and it possesses good link status while minimizing the total path cost. Once, the load is detected by the candidate node, then immediately the packets are fragmented and load is distributed though the selected source node. The selected node is in three useful paths and efficiently distributed the traffic load. Also, for efficient flow distribution a node availability degree standard deviation parameter is decreased the packet drop and increases the packet delivery ratio. In such a way the next implemented phase some error correction techniques such as network coding or forward error correction (FEC) can be implemented in the multipath routing in order to recover the packet losses due to transmission failures.

(Kapil Sharma ,Brijesh Kumar Chaurasia, April 2015)Trust based Location routing is an attractive localized routing scheme for wireless sensor networks (WSNs) due to its desirable scalability and efficiency. Maintaining neighborhood information for the packet forwarding can achieve high efficiency in the geographic routing, but may not be appropriate for WSNs in the highly dynamic scenarios where network topology changes frequently due to nodes mobility and the availability. They proposed a novel online routing scheme, called Energy-efficient Beaconless Geographic Routing (EBGR), which can a provide loop-free, fully stateless, energy-efficient sensor-to-sink routing at a low communication overhead without the help of prior neighbourhood knowledge. In EBGR, each and every node first calculates its ideal next-hop relay position on the straight line towards the sink based on the energy-optimal forwarding distance, and each forwarder selects the neighbour closest to its ideal next-hop relay position as the next-hop relay using Request-To-Send/Clear-To-Send (RTS/CTS) handshaking mechanism. They establish lower and upper bounds on hop count and the upper bound on energy consumption under EBGR for sensor-to-sink routing, assuming no packet loss and no failures in greedy forwarding. Moreover, they demonstrate that the expected total energy consumption along a route towards the sink under EBGR approaches to the lower bound with the increase of node deployment density. They also extend EBGR to the lossy sensor networks to provide energy-efficient routing in the presence of unreliable communication links. Simulation results shows that their scheme significantly outperforms existing protocols in the wireless sensor networks with highly dynamic network topologies. They use a hash function to find locations of the storage nodes, which significantly reduce the storage cost. They also propose a set of similarity threshold functions to the remove outliers from trust opinions. This prevents attackers from generating false trust opinions and from polluting trustworthiness. It allows sensor nodes to put and get the trust data to and from designated storage nodes based on node IDs. Sensor nodes do not need to know the IDs of the storage nodes.

(Hyo Jin Jo ; In Seok Kim ; Dong Hoon Lee June 2017)
Vehicular ad-hoc networks (VANETs) have been researched to be regard to enhance driver's safety and comfort. In VANETs, all the vehicles will share their status and road conditions with neighbouring nodes by periodically generating the safety messages. To provide the reliable VANET services, message authentication is an important feature to be considered. In particular, anonymous message authentication has attracted considerable interest, because periodic broadcast messages from a vehicle can be used to track its location where it is. The proposed anonymous message authentication protocols have been considered serious practical shortcomings, including high communication, authentication, and revocation costs, as well as reliability issues. So, we proposed an anonymous authentication protocol based on a cooperative authentication method. This method does not require mode synchronization between cooperative and non-cooperative authentication. In addition, a two-layer pseudo-identity generation method has been designed and construct a key update tree for efficient revocation.

B. Conclusion

In these existing systems each mobile node is location aware, meaning it knows its location at all times, such as via an on-board GPS unit. Geocast is a network protocol for sending a packet to all nodes within a defined geographic region termed as geocast region. The framework comprises a heuristic-based limited flooding technique, termed as flat geocast that operates within each single tier, a tier being a distinct wireless channel. Typically, distinct tiers will operate at the different transmission ranges for example, in a military scenario; it may be that vehicles have two-tier radios capable both of operating on a short-range channel shared with equipment carried by dismounted soldiers and also of operating on a longer range channel to communicate at distance to other vehicles or buildings.

C. Collective Summary

In these existing systems each mobile node is location aware, meaning it knows its location at all times, such as via an onboard GPS unit. Geocast is a network protocol for sending a packet to all nodes within a defined geographic region termed as geocast region. The framework comprises a heuristic-based limited flooding technique, termed as flat geocast, that operates within each single tier, a tier being a distinct wireless channel. Typically, distinct tiers will operate at the different transmission ranges for example, in a military scenario; it may be that vehicles have two-tier radios capable both of operating on a short-range channel shared with an equipment carried by dismounted soldiers and also of operating on a longer range channel to communicate at distance to other vehicles or buildings.

III. PROPOSED SYSTEM

Our proposed system contains a secure inter-vehicular protocol to disseminate accident warnings, resilient against the position cheating attack. This proposed a new combined architecture of V2V communication, delay tolerant network and V2I communication for large scale data dissemination in VANETs. The aim is to compensate disconnections and network partitioning. A hybrid approach on message propagation is proposed in low density vehicular networks.

A. Architecture

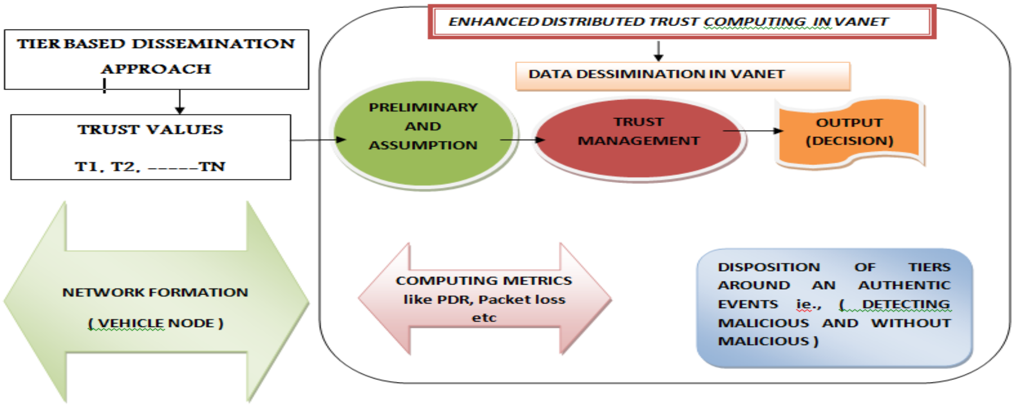

TIER BASED DISSEMINATION APPROACH
TRUST VALUES
T1, T2, -----TN
NETWORK FORMATION
(VEHICLE NODE)
ENHANCED DISTRIBUTED TRUST COMPUTING IN VANET
DATA DESSIMINATION IN VANET
PRELIMINARY AND ASSUMPTION
TRUST MANAGEMENT
OUTPUT (DECISION)
COMPUTING METRICS like PDR, Packet loss etc
DISPOSITION OF TIERS AROUND AN AUTHENTIC EVENTS ie., (DETECTING MALICIOUS AND WITHOUT MALICIOUS)

Figure 1. Enhanced Distributed Trust Computing

1) Node Creation: **VANET uses each and** every participating car into a wireless router or **node**, allowing **them** approximately 100 to 300 meters of each other to connect and **create** a network with a wide range.

2) Get Traffic Data: Vehicular Ad Hoc Network (**VANET**) is an evolving technology in the today's world. The vehicles in **VANET** are considered to be nodes possess mobility as well as computational processing power. Here we discuss about solving **Traffic** Congestion as an application of **VANET**.

3) Data Analysis: Data analysis can be defined a process of inspecting, transforming, and modelling data for discovering useful information, informing conclusions, and supporting decision-making.

4) Trust Establishment Mechanism: Vehicular Ad-hoc networks (**VANETs**) must require trusted vehicles to vehicles communication. **VANET** is multidimensional network in which all the vehicles continuously changing their locations. Secure routing is imperative during the routing process to incorporate mutual **trust** between those nodes.

5) Detect the malicious node behavior based on TMD: **Malicious Node Detection** on Vehicular Ad-Hoc Network Uses Dempster Shafer Theory for Denial of Services Attack. **VANET** is the network which monitoring the traffic on the road and shares the information with neighbors. Movable **nodes** (vehicle) and fixed **node** (RSU) are used in **VANET**.

B. Working Process of proposed System

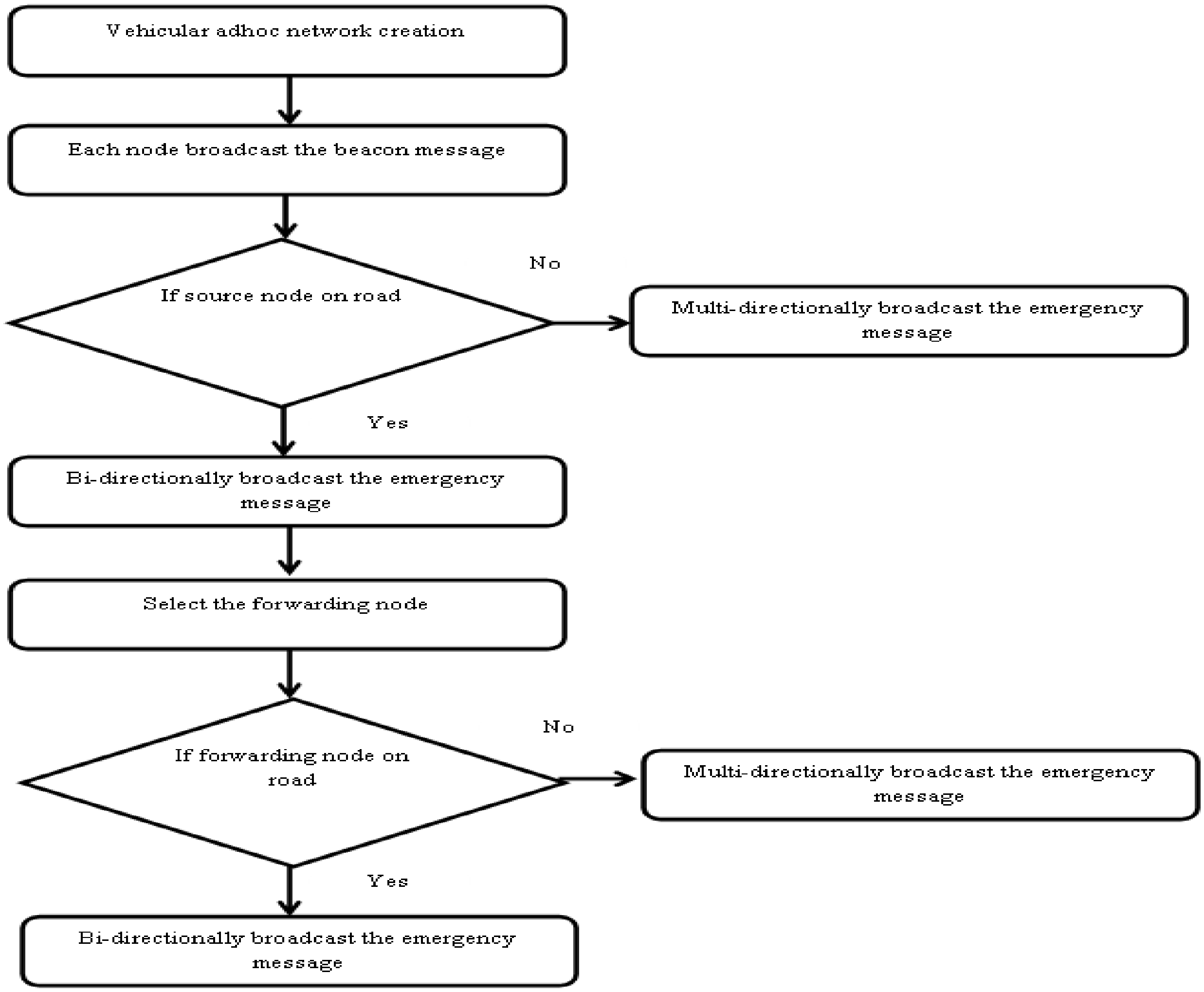

Vehicular adhoc network creation
Each node broadcast the beacon message
If source node on road
No
Multi-directionally broadcast the emergency message
Yes
Bi-directionally broadcast the emergency message
Select the forwarding node
If forwarding node on road
No
Multi-directionally broadcast the emergency message
Yes
Bi-directionally broadcast the emergency message

Figure 2. Flow Process of proposed System

C. Expected Outcomes

They proposed a secure inter-vehicular protocol to disseminate accident warnings, resilient against the position cheating attack. This proposed a new combined architecture of V2V communication, delay tolerant network and V2I communication for large scale data dissemination in VANETs. The aim is to compensate disconnections and network partitioning. A hybrid approach on message propagation is proposed in low density vehicular networks.

D. Metrics

- Packet delivery Ratio(PDR)
- Packet Drop
- Packet Delay
- Throughput
- Energy Consumption

E. Algorithm Used

- A N-Tier based alerts dissemination approach
- Greedy Perimeter Stateless Routing Protocol
- Threshold based malicious node detection algorithm

IV. IMPLEMENTATION AND RESULT

A. Topology Formation

Network topology is the interconnected pattern of network elements. A network topology may be physical, mapping hardware configuration, or logical, mapping the path that the data must take in order to travel around the network.

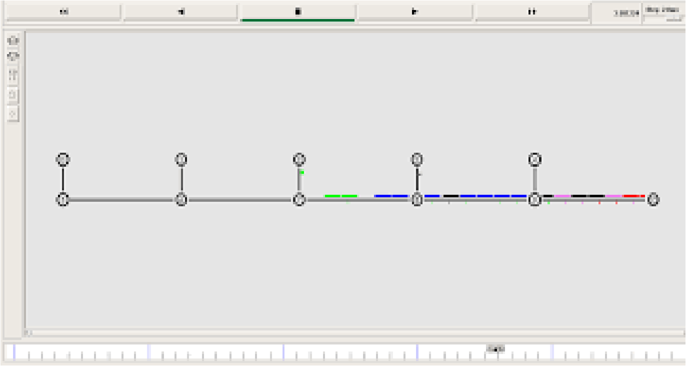


Figure 3. Simulation of Nodes

Constructing project design in NS2 should takes place. In this phase, every node in the ad hoc network communicates with its direct neighbours within its radio range for anonymous neighbour establishment.

B. Neighbor Discovery Phase

Neighbour Discovery Phase are used by nodes to respond to a Neighbour Solicitation message. Routers may inform hosts of a better first hop router for a destination.

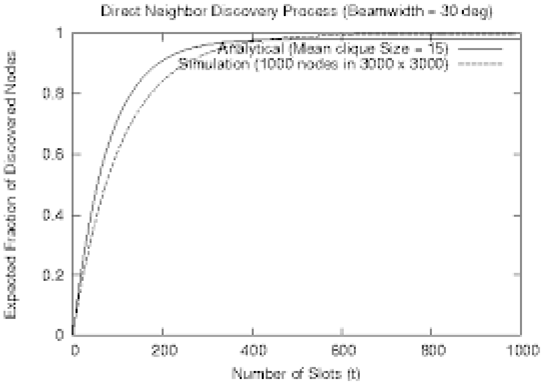


Figure 4. Graph representation of node discovery

This phase is neighbour discovery phase, each source node identifies its neighbour nodes through broadcasting hello packets, through this process each node detects its neighbour nodes corresponding to location and distance. Based on the neighbour discovery phase each node forms a stable path to destination.

C. Data Dissemination

A data dissemination is a process by which data and queries for data are routed in the sensor network.

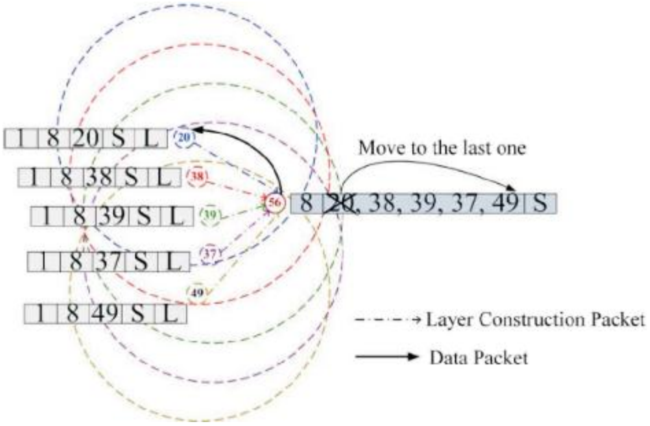
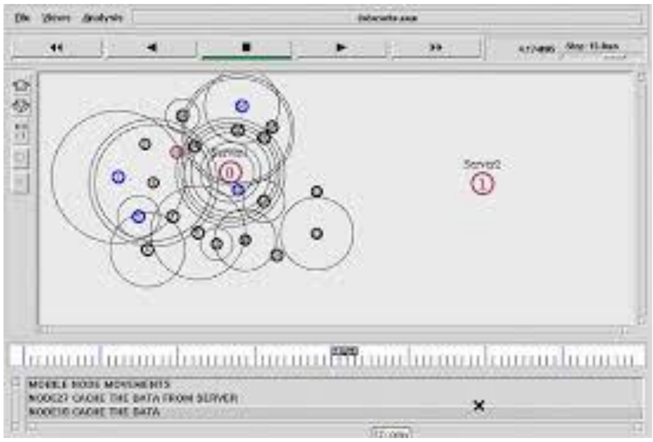


Figure 5. Broadcasting of messages

The source node broadcast the RREQ message to neighbors for establishing the path to destination. The malicious nodes node sends the false RREP message continuously faster than its first source neighbors, at this point source node checks its routing table and performs ECC scalar multiplication process and identifies it's a malicious node and updates its block table that node is a malicious node.

D. Data Transmission

Data transmission is the process of sending digital or analog data over a communication medium to one or more computing, network, communication or electronic devices.



MOBILE NODE MOVEMENTS
NODE27 CACHE THE DATA FROM SERVER
NODE16 CACHE THE DATA

Figure 6. Signal Transmission of each nodes

After the source node S successfully finds out a route to the destination source node S successfully finds out a route to the destination node D, S can start data transmission under the security factor.

E. Graph Design Based Result

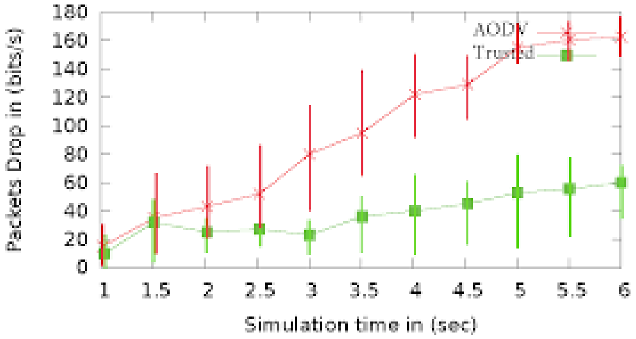


Figure 7. Simulation Results of Packets Drop

Graph is an essential part of display a result, so we plot a graph to show a various result comparison with packets, throughput, energy efficient and etc.

Advantages

- Reactive routing protocols have no need to periodically flood the network for updating routing tables like table-driven routing protocols do.
- Intermediate nodes are able to utilize Route Cache information efficiently to reduce the control overhead.
- The initiator only tries to find a when a route (path) if actually no route is known (in cache).
- Current and bandwidth saving because there are no hello messages needed (beacon-less).

V. CONCLUSION

We proposed a new trust computing protocol called EDTCP for VANETs. The aim is to monitor vehicles behaviour in order to detect the largest set trusted vehicles. Furthermore, we proposed a new data dissemination technique based on tiers in order to mitigate the impact of vehicles misbehaviour, and detect virtually all malicious vehicles. In the proposed framework, each vehicle checks the authenticity of the messages received from its neighbourhood, and then assigns to the transmitter a trustmetric.

REFERENCES

[1] Z. Fei, B. Li, S. Yang, C. Xing, H. Chen, and L. Hanzo, "A survey of multi-objective optimization in wireless sensor networks: Metrics, algorithms, and open problems," IEEE Communications Surveys Tutorials, vol. 19, no. 1, pp. 550–586, Firstquarter 2017.

[2] L. M. Borges, F. J. Velez, and A. S. Lebres, "Survey on the characterization and classification of wireless sensor network applications," IEEE Communications Surveys Tutorials, vol. 16, no. 4,pp. 1860–1890, Fourthquarter 2014.

[3] H. Karl and A. Willig, Protocols and architectures for wireless sensor networks. Hoboken, NJ: Wiley, May 2005.

[4] A. B. Noel, A. Abdaoui, T. Elfouly, M. H. Ahmed, A. Badawy, and M. S. Shehata, "Structural health monitoring using wireless sensor networks: A comprehensive survey," IEEE Communications Surveys Tutorials, vol. 19, no. 3, pp. 1403–1423, third quarter 2017.

[5] D. N. Sandeep and V. Kumar, "Review on clustering, coverage and connectivity in underwater wireless sensor networks: A communication techniques perspective," IEEE Access, vol. 5, pp.11 176–11 199, 2017.

[6] A. M. Abu-Mahfouz and G. P. Hancke, "Alwadha localization algorithm: Yet more energy efficient," IEEE Access, vol. 5, pp.6661–6667, 2017.

[7] Y. S. Chen, D. J. Deng, and C. C. Teng, "Range-based localization algorithm for next generation wireless networks using radical centers," IEEE Access, vol. 4, pp. 2139–2153, 2016.

[8] A. Alomari, W. Phillips, N. Aslam, and F. Comeau, "Dynamic fuzzy-logic based path planning for mobility-assisted localization in wireless sensor networks," Sensors, vol. 17, no. 8, 2017.

[9] S. Halder and A. Ghosal, "A survey on mobile anchor assisted localization techniques in wireless sensor networks," Wireless Networks, vol. 22, no. 7, pp. 2317–2336, 2016

[10] N. A. Alrajeh, M. Bashir, and B. Shams, "Localization techniques in wireless sensor networks," International Journal of DistributedSensor Networks, vol. 9, no. 6, p. 304628, 2013.

[11] G. Han, J. Jiang, C. Zhang, T. Q. Duong, M. Guizani, and G. K. Karagiannidis, "A survey on mobile anchor node assisted localization in wireless sensor networks," IEEE Communications Surveys Tutorials, vol. 18, no. 3, pp. 2220–2243, thirdquarter 2016.

[12] S. Mirjalili, S. M. Mirjalili, and A. Lewis, "Grey wolf optimizer," Advances in Engineering Software, vol. 69, pp. 46 – 61, 2014.

[13] S. Mirjalili and A. Lewis, "The whale optimization algorithm," Advances in Engineering Software, vol. 95, pp. 51 – 67, 2016.

[14] A. Alomari, F. Comeau, W. Phillips, and N. Aslam, "New path planning model for mobile anchor-assisted localization in wireless sensor networks," Wireless Networks, pp. 1–19, 2017.

[15] D. Koutsonikolas, S. M. Das, and Y. C. Hu, “Path planning of mobile landmarks for localization in wireless sensor networks,” Comput. Commun., vol. 30, no. 13, pp. 2577–2592, Sep. 2007.
[16] Yusuf Perwej “The Hadoop Security in Big Data: A Technological Viewpoint and Analysis”, International Journal of Scientific Research in Computer Science and Engineering, Vol.7, Issue.3, pp.1-14, 2019.
[17] Rucha Pawar, “Wireless Mesh Network Link Failure Issues and Challenges: A Survey”, IJSRNSC, Vol -6, Issue-3, 2018.

Authors Profile

Mr. K. Premkumar pursed Bachelor degree from Adhipara Sakthi Engineering college and Master degree in Computer Science and Engineering from Sathyabama Deemed University, Chennai. He is pursuing his P.hd in the field of Vanet at Manonmaniam Sundaranar University, Tirunelveli. He has 16 years of teaching experience.

Dr R. Baskaran pursed Bachelor degree from Pondicherry University Puducherry and Master degree from Vellore Engineering College. He completed his Reserch work in the field of Inforamtion Retrieval from Anna University, Chennai. He is currently working as Professor in Computer Science and Engineering depatment and he has 5 years of Research Experience and 12 years of teaching experience.