International Journal of Innovation Sciences and Research
Vol.5, No, 06, pp. 786-790, June- 2016

Available online at
http://www.ijisr.com

RESEARCH ARTICLE

TRUST FACTOR BASED SECURE CONGESTION CONTROL FOR VANET

[1,*]Shanty Bala and [2]Dr. Vijay Laxmi

[1]Research Scholar M-Tech, Computer Science and Engineering, Guru Kashi University, India
[2]Dean, UCCA, Guru Kashi University, India

Accepted 10th May, 2016; Published Online 30th June, 2016

ABSTRACT

A vehicular ad hoc network, or VANET, is a technology that uses moving cars as nodes in a network to create a mobile network. Vehicular networks are becoming a crucial component for the future intelligent road traffic management system. The key advantages are improved knowledge based real time traffic signaling systems, improved safety of vehicular traffic and reduced vehicular emissions. VANETs can be seen as self-organizing autonomous system which can distribute traffic and emergency information to vehicles in a timely manner. VANET is evolving as one of the practical applications of MANETs in the future. The goal of VANET is to develop a vehicular communication system to provide quick and cost-efficient distribution of data for the benefit of passenger safety and comfort. The key difference of VANET and MANET is the special mobility pattern and rapidly changeable topology. It is not effectively applied the existing routing protocols of MANETs into VANETs. In this investigation, we mainly survey new routing results in VANET. With the consideration of multi-hop forwarding and carry-and-forward techniques, min-delay and delay-bounded routing protocols for VANETs is discussed. The key challenge is to overcome these problems to provide routing protocols with the low communication delay, the low communication overhead, and the low time complexity. The challenges, application, attacks and perspectives of routing protocols for VANETs are finally discussed.

Key Words: Mobile Networks, Vehicular Traffic, MANETS, Vanets.

INTRODUCTION

A vehicular ad hoc network, or VANET, is a technology that uses moving cars as nodes in a network to create a mobile network. A VANET turns every participating car into a wireless router or node, allowing cars approximately 100 to 300 meters of each other to connect and, in turn, create a network with a wide range. As cars fall out of the signal range and drop out of the network, other cars can join in, connecting vehicles to one another so that a mobile Internet is created. It is estimated that the first systems that will integrate this technology are police and fire vehicles to communicate with each other for safety purposes. Vehicular networks have been developed to improve the safety, security and efficiency of the transportation systems and enable new mobile applications and services for the travelling public. Vehicular networks are becoming a crucial component for the future intelligent road traffic management system. Future intelligent road traffic management systems are expected to offer several key advantages compared to the current traffic management systems. The key advantages are improved knowledge based real time traffic signaling systems, improved safety of vehicular traffic and reduced vehicular emissions. Researchers in communications engineering and traffic management systems are engaged for more than a decade to develop suitable Vehicular Ad hoc Networks (VANET) for traffic safety systems.

Corresponding author: Shanty Bala,
Research Scholar M-Tech, Computer Science and Engineering, Guru Kashi University, India.

VANETs can be seen as self-organizing autonomous system which can distribute traffic and emergency information to vehicles in a timely manner. VANETs have several advantages over the conventional wireless networks such as UMTS, LTE and Wi-MAX networks. Main advantages are low cost of implementation and maintenance, self- organization and lower local information dissemination time. VANET is evolving as one of the practical applications of MANETs in the future. This vehicular network is interconnected with vehicles which have wireless interface. The vehicle can easily provide the required power for wireless communication, and adding antennas or additional communication hardware does not cause major problems. The goal of VANET is to develop a vehicular communication system to provide quick and cost-efficient distribution of data for the benefit of passenger safety and comfort. Vehicular delay-tolerant networks rely on opportunistic contacts between network nodes to deliver data in a store carry – and - forward DTN paradigm that works as follows. A source node originates a data bundle and stores it using some form of persistent storage, until a communication opportunity (i.e., a contact) arises. This bundle may be forwarded when the source node is in contact with an intermediate node that can help bundle delivery. Afterwards, the intermediate node stores the bundle and carries it until a suitable contact opportunity occurs. This process is repeated and the bundle will be relayed hop by hop until reaching its destination (eventually and over time).

DIFFERENCE BETWEEN MANET AND VANET

The main differences between VANET and MANET are

Mobility Model – When a vehicle travelling on the road of a city or a freeway, its mobility pattern must consist with the topology of the road. We call this constraint as Mobility In addition; the behaviours of drivers are different to each other, so we can't just use the Random Waypoint mobility model to simulate the movement pattern of vehicles in VANET, Dynamic Mobility and High Relative Speed – In general case, the moving speed of the vehicle is up to 60 – 130km/hr. And the relative speed of vehicles will be higher, especially when moving in the different direction

LITERATURE SURVEY

Ghaleb et al., discussed about mobility pattern based misbehavior detection approach in VANETs. According to this paper the attackers can be classified as insider and outsider. Insider is a legitimate node might intentionally or unintentionally make unauthorized or undesirable actions (Misbehavior), such as modify, fabricate, drop the messages in addition to, impersonate other node identities. Outsider, on the other hand, is a kind of intruder aim to intercept, misuse ordinal of the communications among VANET's nodes. Misbehavior in VANETs can be viewed two perspectives: (i) physical movement and (ii) information security perspectives. Anonymous Location-Aided Routing for MANET (ALARM) is used for vehicular network which relies on the location information and corresponding time. This paper includes algorithms by which the misbehavior can be detected. Sharma et al., proposed various type of security problems and challenges of VANET been analyzed and discussed; author of this paper also discuss a set of solution to solve these challenges and problems. According to this paper each vehicle has OBU (On Board Unit).this unit connects vehicles with RSU via DSRC. and another device is TPD(Tamper Proof Device),this device hold the vehicle secrets like keys, drivers identity, trip detail, route, speed etc. Various attacks discussed are DOS, Fabrication Attack, Alteration Attack, Replay Attack and various attackers are Selfish Driver, Malicious Attackers, and Pranksters.

According to this paper. Various vehicular network challenges are Mobility, Volatility, Privacy VS Authentication, Privacy VS Liability, Network Scalability and various security requirements are Authentication, Availability, Non repudiation, Privacy, Integrity , privacy, Confidentiality. Seuwou et al., proposed about VANET as technology that uses moving cars as nodes in a network to create mobile networks. VANETs enable vehicles to communicate amongst them (V2V communications) and with road-side infrastructure (V2I communications). Every participating car is turned into a wireless router or node, allowing connection between other cars in a radius approximately of 100 to 300 meters, thus creating a network with a wide range. In this paper he proposed various issues of effective security in VANET. He discussed various attacks in VANET, according to him the attacks are classified into two broad categories first one is physical attack which further occur due to two problems ,tamper proof device and event data recorder and another attack is logical attack which occur due to the virus , Trojan horse and protocol weak spot. Qian Yi et al., proposed an overview on a priority based secure MAC Protocol for vehicular networks and he assume that the MAC Protocol can achieve both QOS and security in vehicular networks. In this paper he proposed that the MAC Protocol is having massages with different priority for different application to access DSRC(De dicated short range communication channel) chanel .The proposed secure MAC Protocol will use a part of IEEE 1609.2 .Security infrastructure including PKI and ECC, the secure communication message format of vehicular networks, and the priority based channel access according to the QOS requirement of the applications. Javed et al., proposed the geocasting packet transmission technique to transfer safety message in a vehicular network. He uses OPNET based simulation model to analyze the performance of proposed protocol .According to him the VANET can be seen as self organizing autonomous system which can distribute traffic and emergency information to vehicles in a timely manner. The proposed protocol select the furthest vehicle for the rebroadcast with the help of new back off window design which reduces the number of packet transmission thus lowering the contention levels. The proposed protocol offer very low convergence and warning notification time compared to the other protocols and also generate lower broadcast overhead and packet loss ratio as compared to other protocols.

Hung et al., proposed that additional ad hoc routing protocols are not well suited for these high dynamic network. In this paper they propose a new Heterogeneous Vehicular Network (HVN) architecture and a mobility pattern aware routing for HVN. According to paper HVN integrates Wireless Metropolitan Area Network (WMAN) with VANET technology and reserves advantages of better coverage in WMAN and high data rate in VANET. Vehicles in HVN can communicate with each other and access Internet ubiquitously. They mainly focus on the routing issue for HVN, because the routing protocol for HVN is different from those used in MANET or VANET. They introduce the Mobility Pattern Aware Routing Protocol (MPARP) for HVN to provide more reliable V2V service. According to this protocol the 802.16 is used as the base station which keeps information table The table includes each vehicle's id, current position, and current speed. It will update whenever there is a position update for any of the members in the table.

This protocol uses some format for sending messages. Dias et al., proposed a test bed performance evaluation of DTN-based routing protocols applied to VDTNs(vehicular delay tolerant networks). The objective is to evaluate and understand how popular routing strategies perform in sparse or partitioned opportunistic vehicular network scenarios. This paper based on Spray and Wait protocol. The idea behind using this protocol is to exploit the physical motion of vehicles and opportunistic contacts to transport data between disconnected parts of the network. According to proposed protocol the buffer size and bandwidth is reduced because this protocol manages the flooding by sending single copy of message but suffer from long delivery delay. Sumra et al., proposed about trust is key component of security in vehicular application if any component behave unexpectedly then it would be harmful for

Sr. No.	MANET's	VANET's
1.	MANETs are wireless multi-hop networks that lack infrastructure, and are decentralized and self-organizing	IVC systems satisfy all these requirements, and are therefore a special class of MANETs.
2.	While most MANET articles do not address specific applications, the common assumption in MANET literature is that MANET applications are identical (or similar) to those enabled by the Internet.	IVCs have completely different applications. An important consequence of the difference in the applications is the difference in the addressing modes.
3.	Faithful to the Internet model, MANET applications require point-to-point (unicast) with fixed addressing; that is, the recipient of a message is another node in the network specified by its IP address.	IVC applications often require dissemination of the messages to many nodes (multicast) that satisfy some geographical constraints and possibly other criteria (e.g., direction of movement). The need for this addressing mode requires a significantly different routing paradigm
4.	In MANETs, the nodes are assumed to have moderate mobility. This assumption allows MANET routing protocols (e.g., Ad Hoc On Demand Distance Vector, AODV) to establish end-to-end paths that are valid for a reasonable amount of time and only occasionally need repairs.	In IVC applications, it is shown that due to the high degree of mobility of the nodes involved, even multi-hop paths that only use nodes moving in the same direction on a highway have a lifetime comparable to the time needed to discover the path.
5.	In MANETs, the random waypoint (RWP) is (by far) the most commonly employed mobility model.	For IVC systems, most existing literature recognized that RWP would be a very poor approximation of real vehicular mobility; instead, detailed vehicular traffic simulators are used.
6.	In MANETs a significant body of literature is concerned with power-efficient protocols	IVC enjoys a practically unlimited power supply.

Comparison Table of MANETs and VANETs Protocol:

Protocol	**Advantages**	**Disadvantages**
Proactive (MANETs)	Information is always available. Latency is reduced in the network.	Overhead is high; Routing information is flooded in the whole network.
Reactive (MANETs)	Path available when needed overhead is low and free from loops.	Latency is increased in the network.
Hybrid (MANETs)	Suitable for large networks and up to date information available	Complexity increases
Unicast (VANETs)	Realistic traffic flow is needed some times in some protocols. It works for urban and rural environments	Digital map is needed. Path direction is used to forward the packets. lots overheads are required. improve reliability of min-delay unicast routing protocols to simultaneously reduce delivery delay time and the number of packet retransmissions.
Multicast and Geocast (VANETs)	Digital map is not needed, Realistic traffic flow is not needed in all protocols under it, and Path direction is not used to forward the packets. it works for highways environments. It is worth to develop an efficient multicast/geocast routing protocol for comfort applications with delay-constraint and delay-tolerant capabilities with low bandwidth utilization.	Fragmentation solution shows how a protocol overcomes the temporary network fragmentation problem.
Broadcast (VANETs)	Digital map is not needed. Here impacted traffic flow is used. Path direction is not used to forward the packets and works in single or dual directions. it works for highways environments with geographical area.	To develop reliable broadcast routing protocols for comfort applications to ensure that broadcast messages are successfully disseminated to all the other vehicles in a VANET.

other users of the network. In this paper, they are proposed three different trust levels in peer to peer vehicular network. Purpose of proposed trust levels to discuss in detail is the functionality of different component of network which circumvents the attacker and emphasizes the role of trusted users in peer to peer vehicular communication. According to this paper Trust is combination of expectancy, belief in expectancy and willingness to be vulnerable for that belief. This paper divide trust in three levels which are: zero trust level, weak trust level, strong trust level. The existing model in the paper does not perform the adaptive clustering mechanism for the selection of the receivers for the event updates in order to optimize the volume of VANET data. The average sent packets is higher, and hence causes the higher delay in the VANET networks. The issue of higher delay and higher number of packets can be improved in order to place the faster delivery in progress over the communication links over the vehicular ad-hoc networks by using the re-acknowledgement evaluation.

The existing scheme incorporates the authentication scheme for the purpose of VANET node integrity, but it does not evaluate the ingress traffic in order to notify the node behavior which may add the higher flexibility to the congestion control mechanism. The packet level aggregation has been adopted in the existing model and it does not account for the trusted source. The untrusted source or malicious node may use the data aggregation to transport its malicious towards the vehicular network sink nodes which may exploit the whole operation.

PROBLEM STATEMENT

In the existing system, the flexible and secure congestion control mechanism has been incorporated with dynamic attack prevention system in order to mitigate the congestion caused by the attack data in the vehicular ad-hoc networks. The secure congestion control (SCOOL) is not sufficient to provide the required level of security and trust for the data propagation in VANETs.

The SCOOL scheme performs the authentication, but does not ensure the trust levels of the data source, which is why the data propagation might be effectively used to exploit the network. The hacker can inject any kind of malicious data after gaining the successful authentication, which can cause the congestion on the intermediate and end nodes, which can easily exploit the VANET nodes or the road side units (RSU). This must be checked and protected for the busy periods in the networks, because it may help hacker may be used to gain the unauthorized access to the VANET resources. These attacks may result in the sensitive information theft or the brutal attacks on the availability of the resources under attacks. Also the existing model does not protect the VANET in the initial phase of the communication, which adds a wide loophole in the security of the VANETs.

There is no ingress or incoming data scanning on the regional anomaly scanners incorporated on RSU nodes which must be utilized to scan the data for trust factors. In case if the data scanning will be performed using the one VANET anomaly detection in the given cluster, the RSU and VANET node's performance to propagate the event data may go down due to heavy loads of attack data and may cause congestion and force it to shut the operations resulting in the unavailability of the whole cluster nodes for the convergence period. We are proposing the new model to overcome all of the above mentioned shortcomings of the existing systems. The proposed model will use a pre-shared trust information based trusted source evaluation with higher level of nodal integrity for selection of trusted source's data only. The proposed model will use the dynamic information exchange scheme for the highly trusted communication between the VANET nodes and the region Road Side Unit using the concept of trusted source aware regional anomaly detectors (RADs) implemented over the RSUs. The RAD nodes will form the secure RAD network in order to control the security in the VANET clusters. The RAD nodes will be the nodes with the multiple connections with the other RAD nodes. The RAD nodes will be indulged into the well connected formation for the highly trusted data propagation methods along with the pre-propagation analysis to prevent the malicious data from entering the malicious data for exploitation

APPLICATIONS FOR VANETs

- Public Safety Applications
- Traffic Management Applications
- Traffic Coordination and Assistance Applications
- Traveller Information Support Applications
- Comfort Applications
- Air pollution emission measurement and reduction
- Law enforcement
- Broadband services
- Congestion detection
- Vehicle platooning
- Road conditions warning
- Collision alert
- Stoplight assistant
- Emergency vehicle
- warning
- Deceleration warning
- Toll collection
- Border clearance
- Adaptive cruise control
- Drive-through payment
- Merge assistance

A STATIC-NODE ASSISTED ADAPTIVE ROUTING PROTOCOL IN VEHICULAR NETWORKS

Multi-hop routing protocols in vehicular networks, MDDV [VANET'04], VADD [Infocom'06]. It uses geographic routing with two level. Macro level: packets are routed intersection to intersection. Micro level: packets are routed vehicle to vehicle. Under high vehicle densities both MDDV and VADD work well. Under low vehicle densities when a packet reaches an intersection, there might not be any vehicle available to deliver the packet to the next intersection at the moment. MDDV: not considered, VADD: Route the packet through the best currently available path a detoured path may be taken. SADV architecture as follow in below figure:

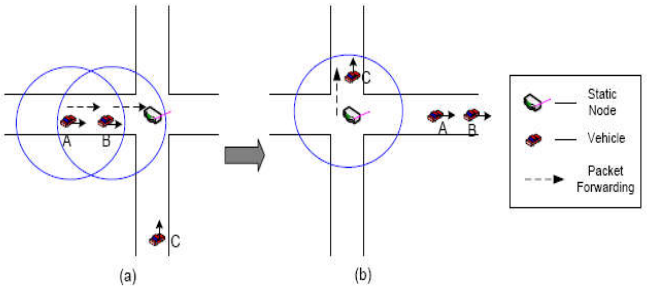

Figure. SADV architecture

A packet in node A wants to be delivered to a destination. The best path to deliver the packet is through the northward road. The packet is stored in the static node for a while the packet is delivered northward when node C comes. Transactions of packets at static nodes, Forward the packet along the best path. If the best path is not available currently, store the packet and wait. Buffer management: Transactions of packets in vehicles along roads, Greedy geographic forwarding used to route the packet to the next static node.

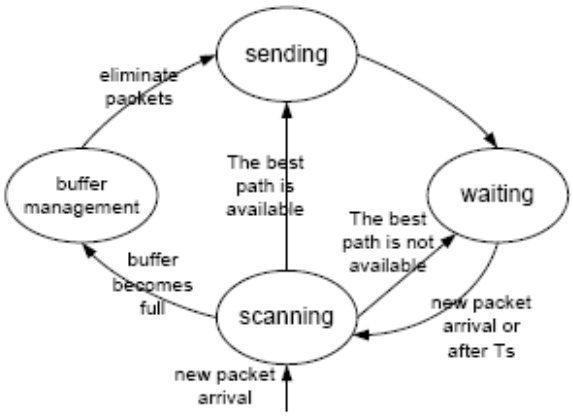

Figure. SADV architecture for nodes transaction Process

ATTACKS

- Sybil attacks,
- Black hole attacks,
- Selective forwarding attacks,
- CTS replay attack

Conclusion

In this paper, we have presented and discussed the taxonomy of routing methods in mobile ad hoc networks and vehicle ad hoc networks comparisons between them is provided. In this survey we reviewed the nature of Geographical Forwarding routing protocols used in multi-hop ad hoc networks. The security of wireless network communication is very important since such a network may be deployed in a crucial environment. To defend against attacks effectively, there is a requirement for GF routing to have defense mechanisms, and to be more resilient to failures. Unicast, multicast, and broadcast routing operations are key issues in the network layer for VANETs. This paper presents a number of routing protocols for MANET, which are broadly categorized as proactive, reactive and hybrid with their advantages and disadvantages as the routing protocols could be chosen.

This work surveys existing unicast, multicast, and broadcast protocols for VANETs. The unicast routing protocols are split into min-delay and delay-bound approaches. The min-delay unicast routing protocols construct a minimum-delay routing path as soon as possible. The delay-bound routing protocol utilizes the carry-and-forward technique to minimize the channel utilization within a constrained delay time. This work also surveys important multicast and geocast protocols for VANETs. The multicast in VANETs is defined by delivering multicast packets from a mobile vehicle to all multicast member vehicles. The geocast in VANETs is defined by delivering geocast packets from a source vehicle to vehicles located in a specific geographic region.. We predict the tendency of the design of routing protocols for VANETs must be the low communication overhead, the low time cost, and high adjustability for the city, highway, and rural environments.

REFERENCES

Chen, Lu, Hongbo Tang, and Junfei Wang. 2013. "Analysis of VANET security based on routing protocol information." In *Intelligent Control and Information Processing (ICICIP), 2013 Fourth International Conference on*, pp. 134-138. IEEE.

Dias, João A., João N. Isento, Vasco NGJ Soares, Farid Farahmand, and Joel JPC Rodrigues. 2011."Testbed-based performance evaluation of routing protocols for vehicular delay-tolerant networks." In *GLOBECOM Workshops (GC Wkshps), 2011 IEEE*, pp. 51-55. IEEE.

Ghaleb, Fuad A., M. A. Razzaque, and Ismail Fauzi Isnin.2013. "Security and privacy enhancement in VANETs using mobility pattern." In *Ubiquitous and Future Networks (ICUFN), 2013 Fifth International Conference on*, pp. 184-189. IEEE.

Hung, Chia-Chen, Hope Chan, and EH-K. Wu. 2008."Mobility pattern aware routing for heterogeneous vehicular networks." In *Wireless Communications and Networking Conference, 2008. WCNC 2008. IEEE*, pp. 2200-2205. IEEE, 2008.

Javed, Muhammad A. and Jamil Y. Khan. 2011."A geocasting technique in an IEEE802. 11p based vehicular ad hoc network for road traffic management." In*Australasian Telecommunication Networks and Applications Conference (ATNAC), 2011*, pp. 1-6. IEEE, 2011.

Khabazian, Mehdi, and M. K. Mehmet Ali. 2007. "A performance modeling of vehicular ad hoc networks (VANETs)." In *Wireless Communications and Networking Conference, 2007. WCNC 2007. IEEE*, pp. 4177-4182. IEEE.

Moser, Steffen, Simon Eckert, and Frank Slomka. 2012."An approach for the integration of smart antennas in the design and simulation of vehicular ad-hoc networks." In *Future Generation Communication Technology (FGCT), 2012 International Conference on*, pp. 36-41. IEEE.

Qian, Yi, Kejie Lu, and Nader Moayeri. 2008. "Performance evaluation of a secure MAC protocol for vehicular networks." In *Military Communications Conference, 2008. MILCOM 2008. IEEE*, pp. 1-6. IEEE.

Samara, Ghassan, Wafaa AH Al-Salihy, and Sures, R. 2010. "Security issues and challenges of vehicular ad hoc networks (VANET)." In *New Trends in Information Science and Service Science (NISS), 2010 4th International Conference on*, pp. 393-398. IEEE.

Sepulcre, Miguel, Javier Gozalvez, Onur Altintas, and Haris Kremo. 2016. "Integration of congestion and awareness control in vehicular networks." *Ad Hoc Networks* 37: 29-43.

Seuwou, Patrice, Dilip Patel, Dave Protheroe, and George Ubakanma. 2012. "Effective security as an ill-defined problem in vehicular ad hoc networks (VANETs)." In *Road Transport Information and Control (RTIC 2012), IET and ITS Conference on*, pp. 1-6. IET.

Sumra, Irshad Ahmed, Halabi Hasbullah, and J.L. A. Manan. 2011. "VANET security research and development ecosystem." In *National Postgraduate Conference (NPC), 2011*, pp. 1-4. IEEE.

Sumra, Irshad Ahmed, Halabi Hasbullah, J. A. Manan, Mohsan Iftikhar, Iftikhar Ahmad, and Mohammed Y. Aalsalem. 2011. "Trust levels in peer-to-peer (P2P) vehicular network." In *ITS Telecommunications (ITST), 2011 11th International Conference on*, pp. 708-714. IEEE.

Younes, Maram Bani, and Azzedine Boukerche 2015. "Scool: A secure traffic congestion control protocol for VANETs." In *Wireless Communications and Networking Conference (WCNC), 2015 IEEE*, pp. 1960-1965. IEEE.

****