Misbehavior Nodes Detection in VANET Using Watchdog Techniques

S. Raagavi
Department of Computer Science
Periyar University
Salem, India
raagavisargunam12@gmail.com

S. Sathish
Department of Computer Science
Periyar University
Salem, India
sathishkgm@yahoo.com

***Abstract*--- VANET is a subset of Mobile Ad- hoc Networks (MANET) in which communication nodes are mainly vehicles. VANET$_S$ enable wireless communication between vehicles and vehicle to infrastructure. Its main objective is to render safety, comfort and convenience on the road. VANET is different from ad-hoc networks due to its unique characteristics. VANET being an ad-hoc network are at risk of various misbehaviors like tampering of messages, eavesdropping, spamming, masquerading it's because of the lack of centralized administration. Security of VANET has been identified as one of the major challenges. In order to do the watchdog correctly and effectively, it must follow the security requirements such as integrity, confidentiality, privacy, non reputation and authentication to protect against attackers and malicious vehicular nodes. Vehicular ad-hoc network relies on cooperation between vehicles and implemented the main techniques for watchdog used to detect the misbehavior node on vehicular communication. A misbehaving node may use to watchdog techniques transmit false alerts, tamper messages, create congestion in the network drop, delay and duplicate packets. Thus detecting misbehaving nodes in VANET is very crucial and indispensable as it might have disastrous consequences.**

Keywords: VANET, MANET, Watchdog, Security, Misbehavior.

1. INTRODUCTION

Vehicular Ad hoc Network (VANET) are created by applying the principles of Mobile Ad hoc Networks (MANETs) the spontaneous creation of a wireless network for data exchange to the domain of vehicles. VANETs were first mentioned and introduced in 2001 under "car to car ad hoc mobile communication and networking" applications, where networks can be formed and information can be relayed among cars. It was shown that vehicle-to-vehicle and vehicle-to-roadside communications architectures will co-exist in VANETs to provide road safety, navigation, and other roadside services. VANET are a key part of the intelligent transportation systems (ITS) framework. Sometimes, VANET are referred as Intelligent Transportation Networks (Hasrouny H, Bassil C, Samhat A, Laouiti A. 2015).

1.1. Security Issues

The use and integration of security mechanisms for warning messages and safety services is absolutely necessary within VANET. The ongoing Network On Wheels (NOW) project addresses a number of security issues in vehicular networks. The project adopts an IEEE 802.11 standard for wireless access and aim at implementing a reference system. The project addresses a number of security issues for VANET. VANET security should satisfy following points (Ghassan, Abdalla, Mosa Ali Abu-Rgheff and Sidi Mohammed Senouci, 2014).

a. Authentication: vehicle reactions to events should be based on legitimate messages (i.e., generated by legitimate senders). Therefore we need to authenticate the senders of these messages.
b. Verification of date consistency: The legitimacy of messages also encompasses their consistency with similar ones (those generated in close space and time) because the sender can be legitimate while the message contains false data(Preetida Vinayakray-jani, 2002).
c. Availability: Even assuming a robust communication channel, some attacks (e.g., DoS by jamming) can bring down the network. Therefore, availability should be also supported by alternative means.

d. Non-repudiation: Drivers responsible for accidents should be deny reliably identified; a sender should not be able to deny the transmission of a message. It may be crucial for investigation to determine the correct sequence and content of message exchanged before the accident.
e. Privacy: People are increasingly wary of enabling technologies. Hence, the privacy of drivers against unauthorized observers should be guaranteed.
f. Real-time constraints: At the very high speeds typical in VANET, strict time constraints should be required

The security issue also includes the following points against which security is needed, these points are given below(Dotzer, 2006).

a) Fake data transmission: The attacker sends false data to modify the behavior to modify the behavior of other vehicles. An example would be sending fake accident warnings to free the road.
b) Masquerading: In this case, the attacker uses a fake identify to escape liability, and place the blame on someone else.
c) Tracking: The attacker here listens for messages coming from a targeted node, and is thus able to monitor the targets movements.

1.2. Vehicular Communication

Rapid advances in wireless technologies provide opportunities to utilize these technologies in support of advanced vehicle safety applications. In particular, the new Dedicated Short Range Communication (DSRC) offers the potential to effectively support vehicle-to vehicle and vehicle-to-roadside safety communications, which has become known as Vehicle Safety Communication (VSC) technologies. DSRC enables a new class of communication applications that will increase the overall safety and efficiency of the transportation system. Intelligent Transportation Systems (ITS) are the future of transportation (Mandala S, 2015)(Li, J. Wu, 2009).

1.2.1. Vehicle to Vehicle Communication

It refers to inter vehicle communication. Vehicles or a group of vehicles connect with one another and communicate like point to point architecture. It proves to be very helpful for cooperative driving.

1.2.2. Vehicle to Infrastructure Communication

Number of base stations positioned in close proximity with a fixed infrastructure to the highways is necessary to provide the facility of uploading/downloading of data from/to the vehicles. Each infrastructure access point covers a cluster.

1.2.3. Cluster to Cluster Communication

In VANETs network is split into clusters that are self managed group of vehicles. Base Station Manager Agent (BSMA) enables communications between the clusters. BSMA of one cluster communicates with that of other cluster.

1.2.4. Security of VANET

In VANET greedy drivers or the other adversaries can be condensed to a greater extent by authentication mechanism that ensures that the messages are sent by the actual nodes. Authentication, however, increases privacy concerns, as a basic authentication scheme of connecting the identity of the sender with the message. It, therefore, is absolutely essential to validate that a sender has a certain property which gives certification as per the application. For example, in location based services this property could be that a vehicle is in a particular location from where it claims to be

- Message integrity
- Message non reputation
- Access control
- Privacy
- Real time guarantees

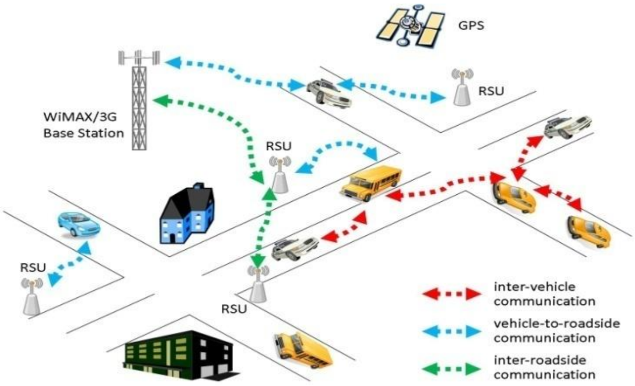
GPS
RSU
WiMAX/3G
Base Station
RSU
RSU
RSU
inter-vehicle communication
vehicle-to-roadside communication
inter-roadside communication

Figure 1. Inter Vehicular communication

1.3. Overview of Watchdog

A Watchdog is a device used to protect a system from specific software or hardware failures that may cause the system to stop responding. The application is first registered with the watchdog device. Once the watchdog is running on your system the application must periodically send information to the watchdog device. It also including for watchdog timer defined for sometimes called a computer operating properly or COP timer, or simply a watchdog is an electronic timer that is used to detect and recover from computer malfunctions, Example concluding for ATM process. Watchdog technique is a fundamental building block to many trust systems that are designed for securing wireless sensor networks (WSNs) (Tarun Varshnay, Tushar sharmea, Pankaj Sharma, 2014).

A Watchdog Timer (WDT) is a hardware timer that automatically generates a system reset if the main program neglects to periodically service. It is often used to automatically reset an embedded device that hangs because of a software or hardware fault as Shown in figure. Watchdog is an application that can 'watch' other applications to ensure they are actively running. If an application should shutdown abnormally or become hung, Watchdog can restart this application. Watchdog is an optional purchase item that can be associated with drop box and Gateway. Watchdog utilizes a heartbeat between the target application and itself (Christofer de Oliveira, Letícia Bolzani Poehls, 2015).

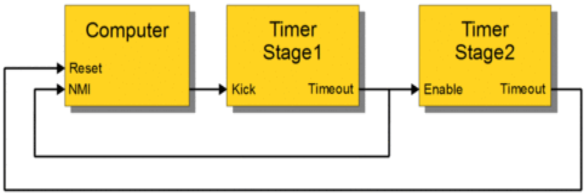

Figure 2. Watchdog Timer

If the target application cannot 'respond' to the heartbeat, Watchdog will restart the program. An example would be if the target program were 'Not Responding'. Watchdog also monitors an EXIT file. When the target application is exited normally, that program will create an EXIT file. Presence of this file allows Watchdog to determine if the closure of the program was intentional. The target application should exit from an error; the EXIT file is not created. At this point, Watchdog will restart the program (Nidhi La, Shishupal kumar, Aditya Saxena, 2015).

Watchdog will not be able to monitor any generic process for drop box and gateway can be monitored. Watchdog only monitors target application on the machine for which it is being run. Watchdog will not monitor a process on another workstation. The Watchdog screen displays the current status of all Target applications. This is not an easy task since nodes may diverge from the protocol due to a selfish behavior or to maintain their data or resources integrity. This paper proposes a cooperative watchdog system to detect and act against misbehavior nodes in order to reduce their impact in the overall network performance (E. O. Ochola, M. M. Eloff, and J. A. van der Poll, 2013).

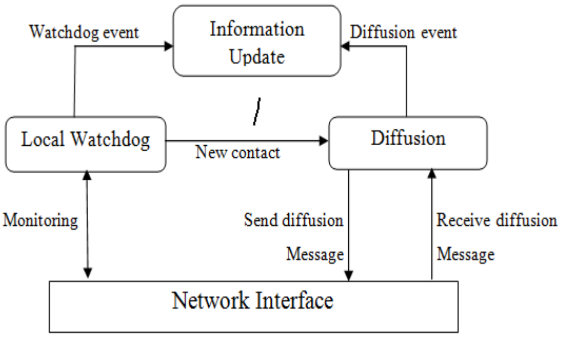

Figure 3. Overview of Watchdog

2. LITERATURE SURVEY

Jay Rupareliya, Sunil Vithlani, Chirag Gohel, (Jay Rupareliya, Sunil Vithlani, Chirag Gohel, 2016) VANET are widely used for comfort and safety applications. Authentication of data is important in this kind of application. So security is one of the important factors in VANET. Different kinds of attacks are there in VANET and different techniques are also there to detect and prevent this attack. This paper will identified attacker using watchdog and apply Bayesian filter to avoid/reduce false positive of node, recognized by watchdog. Misbehaving of nodes is identified by the watchdog, while path rater avoids routing packets through nodes. Each node has its Watchdog. Watchdog is used to verify that next node on the path also forward the packets. By listening the transmission of next node watchdog can detect that whether it is misbehaving or not. If it does not transmit the Packets then it are misbehaving.

Omar Abdel Wahab, Hadi Otrok, Azzam Mourad, (Omar abdel wahab, Hadi otrok, Azzam Moured, 2014) In this proposed method, address the problem of detecting misbehaving vehicles in Vehicular Ad Hoc Network (VANET) using Quality of Service Optimized Link State Routing (QoS-OLSR) protocol. A vehicle is considered as selfish or misbehaving once it over-speeds the maximum speed limit or under-speeds the minimum speed limit where such a behavior will lead to a disconnected network. To detect misbehaving vehicles, cooperative watchdog model based on Dempster–Shafer is modeled where evidences are aggregated and cooperative decision is made. Simulation results show that the proposed detection model is able to increase the probability of detection, decrease the false negatives, and reduce the percentage of selfish nodes in the vehicular network, while maintaining the Quality of Service and stability.

Zhou Wang And Chunxiao Chigan, (Zone wang and chunxiao chigan, 2006) Proposed a cooperation enhancement mechanism using “Neighborhood Watchdog” to generate “Trust Token” based on the first-hand observation. Therefore, trust relationships and packet-acceptance decisions of the receiving nodes are based on the instant observation and the token-proved relaying behavior of the benign neighboring vehicles. As a network layer solution, the cooperation enhancement mechanism proposed in this paper is built on the top of previous proposed Media Access Control (MAC) protocol: Relative Position Based-MAC (RPB-MAC). Researchers reported in apply the Watchdog mechanism to overhear the forwarding behaviors of the downstream neighboring nodes within the transmission range to detect uncooperative behaviors.

Guanhua Yan, Stephan Eidenbenz, (Guanhua Yan, Stephan Eidenbenz, 2014) proposed a systematic framework called Sim-Watchdog, which leverages temporal similarity inherent in graph-modeled network data for anomaly detection. Apply Sim-Watchdog to dynamic graphs extracted from email communication records in a large research institution and demonstrate its effectiveness for supervised anomaly detection. This work focuses on anomaly detection on dynamic graphs abstracted from data collected from networks or distributed systems. The proposed method in this work, while offering a new perspective into anomaly detection in networks or distributed systems, is not intended to replace, but rather to complement existing approaches in this domain.

Andreas Disterh¨oft, Kalman Graffi, (Andreas Disterhoft, Kaiman Graffi, 2016) Monitoring the global state in peer-to-peer networks through decentralized mechanisms allows targeted optimization and improvement of the peer-to-peer network. However, malicious nodes could aim to distort the process of gathering the global state through monitoring. In this proposed DOMiNo, a security solution for tree-based peer-to-peer monitoring

Watchdog mechanisms. It passively listens to incoming events, e.g. data, and rates its suspiciousness based on outlier detection, structural verification and sanity check mechanisms. Main objective, which is to limit the monitoring error of the desired global view, performed an extensive evaluation. Evaluation shows tolerance with normal fluctuations but effective filtering of outliers, which severely influence the global view. As our watchdog solution neither operates passively, any costs nor create new surface for attacks to the monitoring system. Peer-to-peer (P2P) networks offer many advantages compared to client-server network models.

3. MISBEHAVIOUR DETECTION IN VANET

Important to research work proposes on detecting misbehavior or malicious nodes in VANET for watchdog mechanism. A Number of schemes have been proposed to detect misbehavior in vehicular ad-hoc networks. The misbehavior detection schemes can be broadly into following two types. One is node – centric and Data-centric misbehavior detection schemes. It schemes used to detect the misbehavior node in VANET.

3.1. Misbehavior Detection in VANET

Considering the numerous advantages of vehicular ad hoc networks and also dangerous consequences of misbehaviors nodes, the security between vehicles requires special attention and recognizing misbehavior vehicle, is inevitable. Many researchers have been conducted to detect misbehavior node in VANET and we classify them in two categories following for figure 8.

3.1.1. Node centric misbehavior detection

Node-centric techniques need to distinguish among different nodes using authentication. Security credentials, Digital signatures, etc. are used to authenticate the node transferring the message. Such schemes emphasis on the nodes transmitting the messages rather than the data transferred.

Depending on the way a node behaves and how reliably it transmits the messages, node-centric techniques can be further categorized as behavioral and trust based node-centric techniques. Behavioral schemes works on the concept of observing a node's behavior by some trust worthy nodes and uses a metric that helps to identify how effectively a node behaves. Trust based node-centric schemes judge a node by its behavior in past and present and uses it to obtain the expected future misbehavior. Some of the node centric techniques are discussed below.

Propose and analyzed the performance of a Misbehavior Detection Scheme (MDS) for Post Crash Notification (PCN) application. The propose approach relies on observing the driver's behavior after receiving an alert. Based on other neighborhood or visual inputs, the driver can determine if there is really a crash or if the alert is false. This initial work assumes that even in a false alert, the position information will be correct, which may not be true in practice.

They investigated the design of a MDS that does not require this assumption, hence allowing for a broader and more practical misbehavior model. The malicious vehicles detected using the monitoring process over the VANET, once they are detected, proposed algorithm is applied for the prevention of the same. The detection of malicious vehicles is based on DMV algorithm presented earlier. Node-centric mechanisms require authentication mechanisms to reliably distinguish between different nodes. Many systems achieve this by assuming a trusted third party like a PKI that issues credentials, which are then used to authenticate messages and the corresponding information, using a security mechanism like digital signatures. Node-centric mechanisms can further be divided into

- Behavioral mechanisms
- trust-based mechanisms

Behavioral mechanisms inspect a node's observable behavior (but not the information it is sending) and try to derive a metric that identifies how well a node behaves. For instance, a behavioral mechanism may inspect rates at which a neighboring node sends packets and decide whether a node significantly exceeds a "normal rate," which would then be considered as misbehavior. This approach is particularly common in WSNs, and is sometimes referred to as a Watchdog mechanism. However, attempts have been made to distribute these ideas in such a way that the need for a trusted node is removed, with the goal that a Watchdog mechanism can be used in VANETs.

Trust-based mechanisms inspect the past and present behavior of a node and use this to derive a probability for future misbehavior. The assumption is that a node who behaved correctly in the past is more likely to behave correctly in the future. Essentially, this boils down to some form of reputation management scheme where correct behavior increases the reputation while misbehavior reduces it. These mechanisms are commonly used for reporting and local revocation of nodes in a VANET.

3.1.2. Data centric misbehavior detection

Data-centric approach inspects the data transmitted among nodes to detect misbehavior. It is primarily concerned with linking between messages than identities of the individual nodes. The information disseminated by the nodes in the network is analyzed and compared with the information received by the other nodes, in order to verify the truth about the alert messages received. Thus, any vehicular node which sends some bogus information about different events in the VANETs like fake congestion messages, false location, fake emergency events, accidents, road conditions etc. is considered to be misbehaving. Such misbehaviors are identified through data-centric misbehavior schemes.

Few research contributions to the data centric misbehavior detection scheme are as follows, Investigated the use of correlated information, called “secondary alerts”, generated in response to another alert, called as the“ primary alert” to verify the truth or falsity of the primary alert received by a vehicle. First propose a frame work to model how such correlated second ary information observed from more than one source can be integrated to generate a “degree of belief” for the primary alert.

A rule-based data mining fault detection technique to detect faulty/malicious vehicles in VANETs based on exchanged routine messages. A side advantage of VARM scheme is that correlated information, displayed via association rules, are easy to understand and subsequently easy to log by humans. Machine learning algorithms have been applied in this issue; present a machine learning approach to classify multiple misbehaviors in VANET using concrete and behavioral features of each node that sends safety packets.

A security framework is designed to differentiate a malicious node from legitimate node. They implement various types of misbehaviors in VANET by tampering information present in the propagated packet. These misbehaviors are classified based upon multifarious features like speed-deviation of node, received signal strength (RSS), number of packets delivered, dropped packets etc.A vehicle is considered as selfish or misbehaving once it over-speeds the maximum speed limit or under-speeds the minimum speed limit, where such a behavior will lead to a disconnected network.

To detect misbehaving vehicles, cooperative watchdog model based on Dempster Shafer is modeled where evidences are aggregated and cooperative decision is made. Simulation results show that the proposed detection model is able to increase the probability of detection, decrease the false negatives, and reduce the percentage of selfish nodes in the vehicular network, while maintaining the quality of Service and stability. Identified attacker using watchdog and apply Bayesian filter to avoid reduce false positive of node, recognized by watchdog.

In their schema Watchdog method is used to detect the malicious node but what if the node is actually not a malicious node, To detect that they used Bayesian to check whether the detected node is actually a malicious node or not. The presented cheater detection solution is effective in that it only requires vehicles to communicate with their neighboring vehicles without relying on a centralized controlled congestion detection and prediction system. Presented a Misbehavior Detection Scheme (MDS) and corresponding framework based on the mobility patterns analysis of the vehicles in the vicinity of concerned vehicles.

The problem of detecting malicious vehicles in VANET is challenges one. The propose detection model Watchdog is the basic component for the construction of most of the intrusion detection systems proposed so far for self organizing wireless networking systems like VANETs. The main idea behind watchdog is that, because a node can listen to the packets traversing its neighborhood, it can monitor their activity. Therefore, watchdogs act in promiscuous mode, thus overhearing all next nodes forwarding transmissions. With the information about the neighborhood behavior, the watchdog can deduce if nodes are acting as selfish, black or grey hole routers. The

Watchdog is used as the core component of many intrusion detection system mechanisms, Addressed the problem of detecting misbehaving vehicles in Vehicular Ad Hoc Network (VANET) using Quality of Service Optimized Link State Routing (QoS-OLSR) protocol.

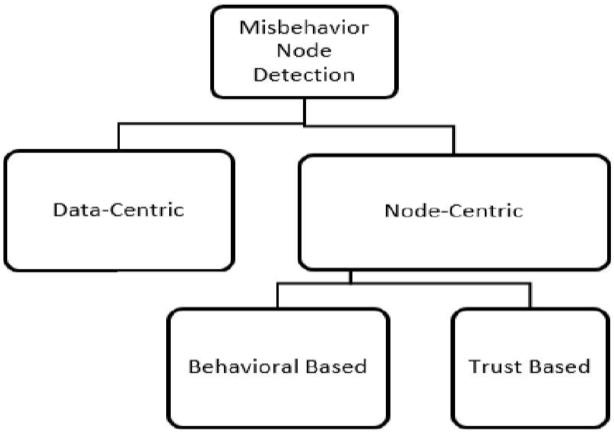

Figure 4. Taxonomy of Misbehavior Detection

4. PROPOSE DETECTING MISBEHAVIOUR NODE ALGORITHM FOR WATDOG TECHNIQUES IN VANET

4. 1. Watchdog Techniques in VANET

Detecting misbehaving of nodes is identified by the watchdog mechanism, while path rater avoids routing packets through nodes. Each node has its Watchdog. Watchdog is used to verify that next node on the path also forward the packets.

By listening the transmission of next node watchdog can detect that whether it is misbehaving or not. If it does not transmit the packets then it is misbehaving. The main aim of this scheme is to detect misbehaving nodes who are not forwarding packets by monitoring neighbor’s node. It also consider path rater component. Benefits of this scheme is it is able detect malicious node in many cases. But the disadvantage of this scheme is it fails to detect malicious nodes in cases of power control employment, partial collusion and collision. Also it fails to control detected malicious nodes. The Watchdog has two functions:

- The detection of selfish nodes
- The detection of new contacts

The local watchdog can generate the following events about neighbor nodes: PosEvt (positive event) when the watchdog detects a selfish node, NegEvt (negative event) when the watchdog detects that a node is not selfish, and NoDetEvt (no detection event) when the watchdog does not have enough information about a node.

The detection of new contacts is based on neighborhood packet overhearing; thus, when the watchdog overhears packets from a new node it is assumed to be a new contact, and so it generates an event to the network information module. The watchdog method detects misbehaving nodes. Figure10 illustrates how the watchdog works. Node A cannot transmit all the way to node C, but it can listen in on node B’s traffic, Thus when A transmits a packet for B to forward to C.

A can often tell if B transmits the packet. If encryption is not performed separately for each link, which can be expensive, then A can also tell if B has tampered with the payload or the header. The implement the watchdog by maintaining a buffer of recently sent packets and comparing each overheard packet with the packet in the buffer to see if there is a match. If so, the packet in the buffer is removed and forgotten by the watchdog, since it has been forwarded on. If the packet has remained in the buffer for longer than a certain timeout, the watchdog increments a failure tally for the node responsible for forwarding on the packet. If the tally exceeds a certain threshold bandwidth, it determines that the node is misbehaving and sends a message to the source notifying it of the misbehaving node.

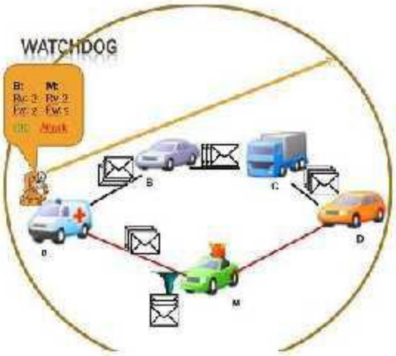

Figure 5. Watchdog mechanism

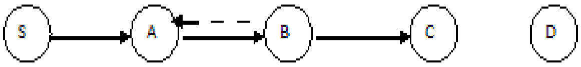

Figure 6. How Watchdog works

4. 2. Detecting misbehavior node algorithm in watchdog

In this thesis propose misbehavior detection algorithm in watchdog techniques for vehicular ad-hoc networks (VANETs), a special case of cyber-physical systems (CPSs).Vehicular ad-hoc networks (VANETs) are networks that are created by equipping vehicles with wireless transmission equipment. VANETs offer great potential to improve road safety and to provide information and entertainment applications for drivers and passengers. Due to the unique properties of VANETs, this type of network has attracted many researchers, including those in the domain of security. The security challenges in VANETs include the requirement for strong privacy, the computationally constrained environment, and the ephemeral nature of connectivity. Evaluate the suitability of existing PKI approaches for insider misbehavior detection and propose a classification for novel detection schemes. The Detection of Misbehavior node algorithm in watchdog is based on the following three basic concepts

- A vehicle is considered to show an abnormal behavior if it drops or duplicate the packets received to it so as to create congestion in the network, misguide other vehicular nodes or destroy crucial messages for their selfish motives.
- An honest vehicle forwards the messages received to it correctly to other nodes in the network or creates right messages for transmission.
- A vehicle will be tagged as a malicious vehicle, if the vehicle repeats abnormal behavior such that its distrust value, D_V exceeds the threshold value T_{MD}.

In VANET communication, a node acts as a source which is the generator of the information. There is another node which acts as a destination of the message, and other intermediate nodes between source and destination acts as relay nodes. When a vehicular node VN plays the role of a relaying node, other trustier vehicles which are its verifiers, monitors its behavior. When vehicle works as a verifier of VN, it checks the number of packets received by VN (represented by parameter a) and number of packets that VN drops or duplicates as detected by VU (represented by parameter b). After a particular time has elapsed PL, if vehicle VN does not send forward a received packet or sends its multiple copies, it is considered as abnormal behavior by verifier VU and hence increases the value of parameter b by 1 unit. The parameter DV (distrust value) is associated with each vehicle and changes when an abnormal behavior is observed. The new distrust value is informed to all neighbors and they update their lists accordingly. Vehicles cooperate with one another while they are part of the white list as their Dv is lower than the threshold. If it exceeds the threshold, the ID of the vehicle is reported to the CA as a malicious node. CA then broadcasts the ID of malicious node to all others nodes.

In watchdog detection of Misbehavior Nodes (DMN) algorithm, verifier is selected on the basis of the parameters: distrust value, load, and distance. Those nodes are selected as verifier whose Decision parameter, DP is less than the Selection Threshold, TVS among other neighboring nodes located in the region r (VN). This approach optimizes the selection of verifier nodes and thus helps to save the network bandwidth and hence improves network performance. Nodes in the region r are considered for being verifiers. The region r denotes the intersection area of vehicular node VN. Area of group of vehicle refers to its transmission range and area of vehicle VN is calculated by the formula given below in Equation (1). Thus it ensures all verifiers are able to send misbehavior reports to the vehicle.

$$\text{Area}\ (V_N) = T_R(V_N) - PL\ (Smx - Smn\ ) \tag{1}$$

where, T_R (V_N) - Transmission range of vehicle $V_{N,}$ P_L- Packet latency in vehicles, Smx- Maximum speed of vehicle, Smn - Minimum vehicle speed

The parameters for selection of verifiers in the area r are explained below:

Load (LD): It refers to the number of nodes, a vehicle s already monitoring. It is considered so as to balance the monitoring job among the nodes. Thus a node which has less load compared to others will have greater chance to be selected as verifier.

Distrust value (DV): It refers to the measure of trustworthiness of a vehicle. It means less the distrust value, more trustworthy a node is. If a vehicle shows abnormal behavior, this value is increased and compared to the threshold for making appropriate decisions i.e. a vehicle should remain in the white list or tagged as a malicious vehicle and moved to the black list.

Distance (DS): If the distance of a node from the vehicle to be monitored is less, then the node will remain in the transmission range of the vehicle for a longer time. Thus, this provides scope for better observations and decision making. Decision Parameter, D_P is calculated for all the nodes considered for verifier selection by taking into account the load, distance and distrust value of the node by the following equation (2),

$$D_P = W_1 * L_D + W_2 * D_V + W_3 * D_S \tag{2}$$

where, W_1, W_2, and W_3 are the weight factors for parameters Load (LD), Distrust Value (DV) and Distance (DS) respectively such that, $W_1 + W_2 + W_3 = 1$

Instead of selecting all the nodes with smaller distrust value than the vehicular node VN, allocating few nodes as verifiers which are more appropriate for monitoring process helps in better detection of malicious nodes as well as improves network performance. As few nodes perform the job of monitoring the node VN, this saves network resources used for reporting the behavior and conserve their time for processing the observed behavior for all the nodes. As the network utilization is enhanced, it results in better transmissions in the network. In order to assign verifiers for the node VN, the decision parameter DP calculated for the nodes under consideration is compared to the selection threshold TVS, if a node's decision parameter value less than the selection threshold (DP< TVS), then the vehicle is allocated as verifier. This way optimizes the selection of verifier nodes.

4. 3. Detecting Misbehavior Node Algorithm in watch dog

```
Step 1: Vehicle $V_N$ joins the vehicular network.
Step 2: Get the keys.
Step 3: Compute the parameters- Load, Distrust Value and Distance for the nodes in area of $V_N$ for verifier selection.
Step 4: Calculate the Decision parameter for verifier selection, $D_P$.
        $D_P = W_1 * L_D + W_2 * D_V + W_3 * D_S$
        Where,
        $W_1 + W_2 + W_3 = 1$.
        W1, W2, and W3 are the weight factors for parameters Load (LD), Distrust Value (DV) and Distance (DS) respectively.
Step 5: Find out nodes with Decision parameter value less then Selection Threshold, i.e ($D_P< T_{VS}$)
Step 6: Allocate nodes obtained from Step 5 as verifiers to the recently joined vehicle $V_N$.

Step 7: Verifiers monitor behavior of vehicle $V_N$.
Step 8: If (verifier detects vehicle $V_N$ showing abnormal behavior)
                Report to the watchdog monitoring vehicle
                goto step 9;
        else
                goto step 7;
Step 9: calculates new distrust value ($D_V$) of $V_N$.
Step 10: If distrust value is less than or equal to detection threshold i.e
        if ($D_V< = T_{MD}$ ) then
                update the white list and goto 7
        else
                goto 11
Step 11: Warning message is send to all other nodes.
Step 12: Update the entry of Vehicle $V_N$ in black list.
Step 13: Isolate the detected misbehavior vehicle from the network.
```

5. EXPRIMENTAL RESULT

Result and Analysis: Performance analysis of AODV, DSDV & DSR work show in the figure and table.

Table 1: Performance Analysis

Analysis	Throughput (Kpbs)	Packet Delivery Ratio (%)	End-to-End Delay (ms)
AODV	314.32	98.64	30.53
DSDV	108.02	78.09	20.40
DSR	336.28	99.78	50.33

6. CONCLUSION AND FUTURE WORK

6. 1. Conclusion

Security is always an open area of research and improvement. The configuration of watchdog security mechanism in vehicular ad hoc network is a challenging task due to its dynamic nature and resource constrain. This work describes how to detect misbehavior node in on the VANET have drastically degraded the network performance. The help of detecting misbehavior node algorithm based on selection verifiers node which perform the work of monitoring node behavior. Detecting misbehavior node algorithm select the entire node as verifiers which have distrust value less than the vehicle to be monitored. It has been obtained by watchdog algorithm taking into consideration in three parameters for choosing appropriate verifiers that are load, distance and distrust value. Watchdog node in the network maintain and monitoring all other vehicle as well as neighboring vehicle for detecting selfish node. Watchdog algorithm is design to isolate the nodes showing abnormal behavior as well as enhancing the network performance.

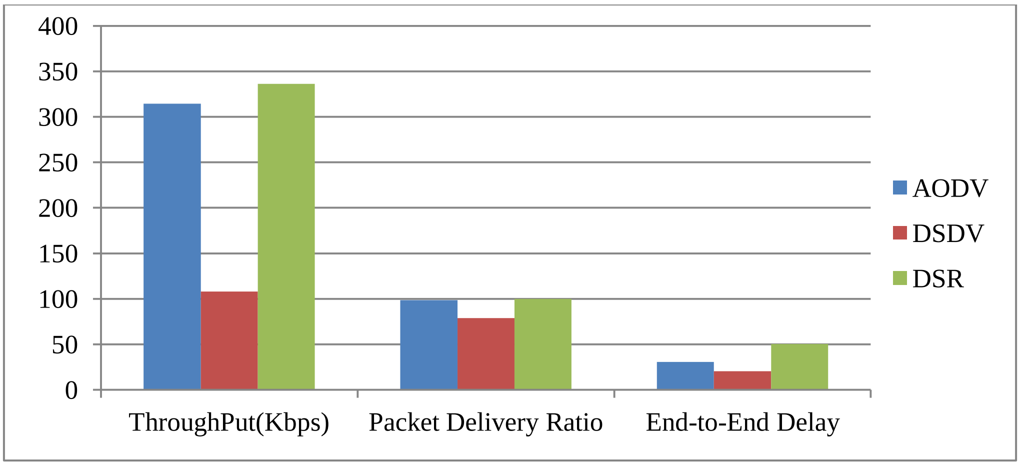

Figure 7. Performance Analysis

6. 2. Future Work

The vehicular Ad hoc network is an open challenging area of research in network due to its dynamic nature. In future plan is to configure this proposed mechanism with other mechanism such as neural network, intrusion detection schemes to identity the misbehavior node in the network. Complex traffic modeling and driving behavior (mobility models) that incorporate lance changing and multiple entry and exit points can be integrated to our simulation framework to validate and evaluate our algorithm in more complex scenarios, taking them closer to real world application.

REFERENCES

Hasrouny H, Bassil C, Samhat A, Laouiti A (2015). Group-based authentication in V2V communications, Fifth International Conferenceon Digital Information and Communication Technology and its Applications (DICTAP), 173–177.

Ghassan, Abdalla, Mosa Ali Abu-Rgheff and Sidi Mohammed Senouci (2014), Current Trends in Vehicular Ad Hoc Network, Mobile Communications Network Research, Protland.

Preetida Vinayakray-jani (2002), Security within Ad Hoc Networks, PAMPAS Workshop

F. Dotzer (2006). Privacy issues in Vehicular ad hoc networks. Lecture Notes in Computer Science, 3856, 197-209.

Mandala S (2015), Trust management in vehicular ad hoc network: a systematic review, EURASIP Journal on Wireless Communications and Networking.

F. Li, J. Wu (2009), Frame: an innovative incentive scheme in vehicular networks", IEEE International Conference on Communications.

Tarun Varshnay, Tushar sharmea, Pankaj Sharma (2014), Implementation of watchdog protocol with AODV in Mobile ad hoc network, Fourth International Conference on Communication Systems and Network Technologies.

Christofer de Oliveira, Letícia Bolzani Poehls (2015), On-Chip Watchdog to Monitor RTOS Activity in MPSoC Exposed to Noisy Environment, 10th International Workshop on the Electromagnetic Compatibility of Integrated Circuits (EMC Compo), Edinburgh, 10–13.

Nidhi La, Shishupal kumar, Aditya Saxena (2015). Detection of Malicious node Dehaviour Via Watchdog protocol in mobile ad hoc network witch DSDV Routing Scheme, Elsevier.

E. O. Ochola, M. M. Eloff, and J. A. van der Poll (2013). The Failure of Watchdog Schemes in MANET Security: A Case of an Intelligent Black-Hole, Proceedings of the SAICSIT 2013 Conference, East London, South Africa.

Jay Rupareliya, Sunil Vithlani, Chirag Gohel (2016). Securing VANET by preventing attacker node using Watchdog and Bayesian Network Theory, 7th International Conference on Communication, Computing and Virtualization.

Omar abdel wahab, Hadi otrok, Azzam Moured (2014). A cooperative watchdog model based on Dempster-Shafer for detecting misbehaving vehicles, Journal of Elsevier.

Zone wang and chunxiao chigan (2006), Cooperation Enhancement for Message Transmission in VANET, Springer.

Guanhua Yan, Stephan Eidenbenz (2014), Sim-Watchdog: Leveraging Temporal Similarity for Anomaly Detection in Dynamic Graphs, 34th International Conference on Distributed Computing Systems, IEEE.

Andreas Disterhoft, Kaiman Graffi (2016), Convex Hull Watchdog: Mitigation of Malicious nodes in Tree-based P2P Monitoring system, IEEE conference on local computer networks.