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

International Journal of Current Research in Life Sciences
Vol. 07, No. 02, pp.1219-1224, February, 2018

ISSN: 2319-9490

RESEARCH ARTICLE

FUZZY DEDUCTION SYSTEM FOR SECURING VANETS USING ATTACK-RESISTANT TRUST MANAGEMENT SCHEME (ART)

***[1]Arpana Singh Kushwaha and [2]Dr. Raghav Yadav**

[1]M.Tech Scholar, Department of CSIT, SHUATS, Allahabad, U.P, India
[2]Associate Professor, Department of CSIT, SHUATS, Allahabad, U.P, India

Received 22nd December, 2017; Accepted 28th January, 2018; Published Online 28th February, 2018

ABSTRACT

VANET has become a live field of study, standardization, and elaboration because it has massive potential to enhance vehicle and road safety, traffic effectiveness, and convenience as well as accommodation to both motorist and passengers. Recent research efforts have placed a strong accent on novel VANET design architectures and implementations. A lot of VANET research work have axis on concrete areas including routing, broadcasting, Quality of Service (QoS), and safety. In VANETs, due to the characteristics such as openness and dynamic topology, networks suffer from various attacks in the data plane. Even worse, some attacks can subvert or bypass the frequently used identity-based security mechanisms. To secure the data plane of VANETs, trust management system was proposed. An attack resistant trust management scheme is capable of detecting malicious attacks and also deals with it. It also calculates the trustworthiness of both data node and mobile node in VANETs. But the issues were that the model is considering trust factor only to find route from source to the destination. The acquired route on the basis of single parameter has proven to be ineffective and less trust worthy. Moreover, the designed system takes decision manually on the basis of threshold value and decision taken manually can be inappropriate at several points. Considering this fact, the existing system is concluded as less trust worthy and ineffective in terms of transmission of data. In this paper, the manual decision making process of ART scheme is replaced with artificial intelligence system i.e. fuzzy deduction system to evaluate the selection rate of individual node in the network. In addition to this, FDS grouping approach is initiated in novel method to group the nodes and based on the maximum selection rate in individual group; a node will be selected for the transmission of data. This criterion will enhance the level of security with reduction in error rate while selecting relay node.

Key words: *VANETs, trust management, artificial intelligent system, FDS algorithm, security, simulation.*

Citation: Arpana Singh Kushwaha and Dr. Raghav Yadav, 2018. "Fuzzy deduction system for securing vanets using attack-resistant trust management scheme (art)" *International Journal of Current Research in Life Sciences*, 7, (02), 1219-1224.

INTRODUCTION

Vehicular Ad Hoc Networks (VANETs) have grown out of the needfulness to support the growing number of wireless products that can now be accustomed in vehicles (Raya and Hubaux, 2005; Harsch *et al.,* 2007). These products contain remote keyless entry devices, personal digital assistants (PDAs), laptops and mobile telephones. As mobile wireless devices and networks become increasingly important, the demand for Vehicle-to-Vehicle (V2V) and Vehicle to-Road side (VRC) or Vehicle-to-Infrastructure (V2I) Communication will continue to grow (Harsch *et al.,* 2007). VANETs can be utilized for a wide range of safety and non-safety applications, permit for value added services such as vehicle safety, automated toll payment, traffic management, enhanced navigation, location-based services such as finding the closest fuel station, restaurant or travel lodge (Gerlach, 2006) and infotainment applications such as providing access to the Internet.

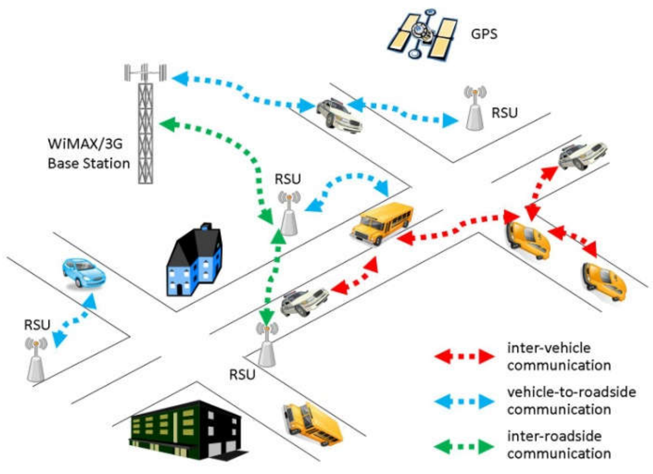

GPS
RSU
WiMAX/3G
Base Station
RSU
RSU
RSU
inter-vehicle communication
vehicle-to-roadside communication
inter-roadside communication

Fig 1. Vehicular Communication Networks

Corresponding author: **Arpana Singh Kushwaha,**
Department of CSIT, SHUATS, Allahabad, U.P, India.

Over the last few years, we have validated many research efforts that have investigated various issues related to V2I, V2V, and VRC areas because of the vital role they are anticipated to play in Intelligent Transportation Systems (ITSs). In fact, different VANET projects have been executed by various governments, industries, and academic institutions around the world in the last decade or so. Security of VANETs has been identified as one of the substantial challenge. VANETs applications support real time communication and deals with life critical information. In order to does it remedy and effectively, it must follow the security conditions such as integrity, confidentiality, privacy, non repudiation and authentication to defend against attackers and malicious vehicular nodes. There are various attacks like black hole, Sybil, DoS, Timing, Illusion etc. which not only influence the driver's and vehicle's privacy but also compromise traffic safety and may lead to loss of life (Raya and Hubaux, 2005; Harsch *et al.,* 2007; Gerlach, 2006; Engoulou *et al.,* 2014). Thus, in order to become a real technology that reassures traffic safety, VANETs needs applicable security methodology and mechanisms that will give surety protection against several misbehaviors and malicious nodes that influence security of VANET. One typical application of VANETs is the Traffic Estimation and Prediction System (TrEPS), which generally gives the predictive information required for proactive traffic control and traveler information (Lin and Song, 2006). Traffic estimation and prediction systems (TrEPS) have the potential to upgrade traffic conditions and decrease travel delays by facilitating better utilization of available capacity.

These systems deed currently available and emerging computer, communication, and control technologies to monitor, handle, and regulate the transportation system. They also deliver different levels of traffic information and trip advisory to system users, including many ITS service providers, so that travelers can make timely and informed travel decisions. The success of ITS technology deployments is heavily dependent on the availability of timely and precise estimates of prevailing and emerging traffic conditions. As such, there is a strong necessity for a "traffic prediction system". The needed system is to use for advanced traffic models to analyze data, especially real-time traffic data, from different sources to estimate and predict traffic conditions so that proactive Advanced Traffic Management Systems (ATMS) and Advanced Traveler Information Systems (ATIS) strategies can be implemented to meet various traffic control, management, and operation objectives. An attack-resistant trust management scheme called *ART* is proposed to cope with malicious attacks and estimate the trustworthiness of data as well as nodes in VANETs (Li and Song, 2015). To secure the data plane of VANETs, trust management system was proposed. But the issues were that the model is considering trust factor only to find route from source to the destination. The acquired route on the basis of single parameter has proven to be ineffective and less trust worthy. Moreover, the designed system takes decision manually on the basis of threshold value and decision taken manually can be inappropriate at several points. Considering this fact, the existing system is concluded as less trust worthy and ineffective in terms of transmission of data. In this research paper, the manual decision making process of the ART scheme is replaced with artificial intelligence system i.e. fuzzy deduction system to evaluate the selection rate of individual node in the network. In addition to this, Fuzzy Deduction System (FDS) grouping approach is initiated to group the nodes and based on the maximum selection rate in individual group; a node will be selected for the transmission of data. This criterion will enhance the level of security with reduction in error rate while selecting relay node. We model and evaluate the trustworthiness of data and node as two separate metrics, namely *data trust* and *node trust*, respectively. In particular, *data trust* is used to assess whether or not and to what extent the reported traffic data are trustworthy. On the other hand, *node trust* indicates how trustworthy the nodes in VANETs are. Moreover, the ART scheme can detect malicious nodes in VANETs. To evaluate the performance of the proposed ART scheme using fuzzy deduction system, extensive experiments have been conducted. Experimental results show that the proposed ART scheme with fuzzy system is able to accurately evaluate the trustworthiness of data and nodes in VANETs, and it is also resistant to various malicious attacks.

The rest of the paper is organized as follows. In Section II, reviews related work is given. Section III describes the basics of the research problem in details. In Section IV, Fuzzy Deduction System is described in detail with Fuzzy deduction grouping approach. Section V presents the experimental study that has been conducted. Finally, the conclusion is drawn in Section VI.

BACKGROUND

In recent years, research communities have directed much concentration to trust management, especially in distributed background such as ad-hoc networks, peer-to-peer networks, and e-commerce markets. Trust management involves two types of entities: a trustor and a trustee. A trustor is the entity who aims to measure the trustworthiness degree of the evaluated entity, i.e., the trustee. The trust evaluation model (trust model) is a set of mathematical methods to calculate the trustworthiness degree. The trust management system is the framework consisting of three interdependent parts: the trust factor collection approach, the trust evaluation model, and the trust-based controlling mechanism. Basically they are related to misbehavior detection. Information dissemination in VAN ETs happens through cooperative behavior of the vehicular nodes. Messages transmitted in vehicular network carry vital information like traffic jam, emergency brake events, road conditions, accident notifications, bad weather conditions, etc. In such a case, if any vehicle act maliciously and tamper with the messages, the results may be very dangerous. Thus misbehaviors in VANET are a very crucial issue. Misbehavior can be generally referred to as any kind of abnormal behavior that is deviation from the average behavior of other vehicular nodes in the VANETs. Hence, detection of misbehaviors and the malicious vehicular nodes involved in such misconducts is extremely imperative, in order to make VANET a secure network. A lot of work has been carried out to detect misbehavior and malicious nodes in Vehicular ad hoc networks. The misbehavior detection schemes can be broadly classified into following types: Node centric and Data-centric misbehavior detection schemes.

In the research work Ghosh et al. (Ghosh *et al.,* 2009; Ghosh *et al.,* 2010) have proposed a robust scheme to detect malicious vehicles for Post Crash Notification application. The approach applied, firstly observes a driver's actions post raising a crash alert message. Observed mobility and expected trajectory of the vehicle for the crash mobility model is calculated and if the difference between the two exceeds a certain threshold value, the alert is considered to be false. The approach effectively reduces the false positives and false negatives while effectively detecting misbehavior. In (Wahab *et al.,* 2014) Ghosh et al. improved their previous work (Kadam *et al.,* 2014) by considering the possibility of the fake position information of the vehicle in the PCN along with the false crash alert. The cause-tree representation is used effectively to conjointly accomplish misbehavior detection in addition to identification of its root-cause by employing logical reduction. The scheme proves to be robust and achieves considerable detection of misbehavior. In the research work, Wahab *et al.* (2014) have used Quality of Service-Optimized Link State Routing (QoS-OLSR) clustering algorithm to detect malicious vehicles in VANET. Certain vehicles may over speed the maximum speed limits or under speed the minimum range, thus may prove to be uncooperative in packet forward and cluster formation resulting in performance degradation of the network. Authors have proposed a two phase model incentive and detection. Vehicles are motivated by giving incentives during formation of clusters. After cluster formation, misbehavior is detected by aggregating evidences and cooperative decision using Dempster–Shafer based cooperative watchdog model. Incentives are in the form of reputation where network services are provided depending on reputation value. Watchdogs are appointed from the nodes in the network that monitor behavior of other nodes in order to ensure vehicles are cooperating with each other. This method maintains stability and Quality of Service with increase in detection probability and decreasing the number of selFDSh nodes and false negatives. Kim and Bae (2012) have proposed a novel misbehavior based reputation management scheme (MBRMS) which includes three components (a) Misbehavior detection (b) Event rebroadcast and (c) Global eviction algorithms for the detection and filtration of false information in VANETs. Each vehicular node maintains information system of events and corresponding actions for the detection of misbehaving node.

The presented mechanism uses outlier detection technique and misbehaving risk value of the bad node to measure the risk level. MBRMS effectively detects and evicts the misbehaving nodes. In the research work, Daeinabi and Rahbar (2013) have proposed the Detection of Malicious Vehicles (DMV) algorithm through observation to discover malicious nodes that drop or duplicate received packets more than a given threshold value. Vehicles are tagged using a distrust value and are monitored by the allocated verifier nodes. Black and white lists are maintained in order to isolate the malicious vehicles from the honest vehicles. It has been observed in simulation that detection of malicious vehicles is faster in case of Constant Speed Motion (CSM) and Smooth Motion Model (SMM) as compared to Fluid Traffic Model (FTM). Performance analysis shows that this misbehavior detection scheme is capable of finding out most existence malicious vehicles even at quite high speeds. Kadam and Limkar (2014) have presented an improvement of the DMV algorithm (Daeinabi and Rahbar, 2013). It not solely detects malicious nodes however additionally their prevention from the VANET. This approach reduced the impact of black hole attack within the VANET and is more efficient and secure compared to DMV.

PROBLEM DEFINITION

In this part, the research problem that is contending in this paper will be portraying in more details, containing the network model as well as the adversary model. In VANETs, data plane has various attacks in network because of openness and dynamic topology. Trust Management System was proposed for securing the data plane of VANETs. There was need to find path from source to destination. For this, this model was considering trust factor only which is an issue. Route found on the basis of single parameter is not effective. And it also cannot be trusted. Also, the designed system was taking decisions manually on the basis of threshold value and decision taken manually can be inappropriate at many points. Considering this fact, the existing system is concluded as less trust worthy and ineffective in terms of transmission of data. For this we are introducing new methods for acquiring routes which can be trusted.

Objectives

The main objectives for the proposed techniques are:

1. To design fuzzy oriented intelligent system for selection of appropriate relay node while transmission of data.
2. To introduce more number of security parameters for advanced level of security in the network.
3. To design enhanced next hop selection mechanism using Fuzzy Deduction grouping approach.
4. To perform comparative analysis between traditional and proposed technique.

Network Model

A VANET commonly refers to a wireless network of miscellaneous sensors or other computing devices that are deployed in vehicles. This kind of network permits uninterrupted monitoring and sharing of route situations and status of the transportation systems. All of the nodes in VANETs are equipped with the same wireless communication interface, such as IEEE 802.11p. The nodes are limited in energy as well as computational and storage capabilities.

Opponent Model

First of all, the RSUs are supposed to be reliable since they are conventionally better protected. The connected vehicles, on the other hand, are commonly more susceptible to different attacks, and they can be accommodated at any time after the VANET is formed. The opponent can be an outsider located in the wireless range of the vehicles, or the adversary can first compromise one or more vehicles and behave as an insider later. The opponent is capable to eavesdrop, jam, modify, forge, or drop the wireless communication between any devices in range. The main goals of the opponent may include intercepting the normal data transmission, forging or modifying data, framing the benign devices by deliberately submitting fake recommendations, etc. More specifically, the following malicious attacks are considered in this paper.

- Simple Attack (SA): An attacker may exploit the negotiated nodes not to succeed normal network protocols and not to deliver needed services for other nodes, such as forwarding data packets or propagating path detection queries. However, the compromised node will not deliver any false trust conviction when it is asked about other node’s trustworthiness.
- Bad Mouth Attack (BMA): In addition to conduct simple attack, the attacker can also circulates false trust conviction and attempt to frame the harmless nodes so that the truly malicious nodes can stay undetected. This attack heads to break the right trust estimation and

make it affectless to successfully distinguish the malicious attackers.

- Zigzag (On-and-off) Attack (ZA): Sometimes sly attackers can change their malicious behavior patterns so that it is even harder for the trust management scheme to identify them. For instance, they can guide malicious behaviors for some time and then halt for a while. In addition, the wily attackers can also display various behaviors to different audiences, which can lead to conflicting trust opinions to the same node among different audiences. Due to the deficient proof to indict the malicious attacker, it is generally more harder to identify such wily attackers.

MATERIALS AND METHODS

Proposed Work

In this section, the proposed Fuzzy deduction system is presented in details. After having a review to the traditional work, it is observed that it has been still poses the backlogs which motivate to develop a new approach in direction of solution to the problem. Initially, security parameters have enhanced which were used to find a route from source to the destination. Including trust parameter as in the existing approach, two more parameters are introduced such as Reputation value and delay factor. The manual decision making process is replaced with artificial intelligence system i.e. fuzzy deduction system to evaluate the selection rate of individual node in the network. In addition to this, Fuzzy deduction grouping approach is initiated in novel method to group the nodes and based on the maximum selection rate in individual group; a node will be selected for the transmission of data. This criterion will enhance the level of security with reduction in error rate while selecting relay node.

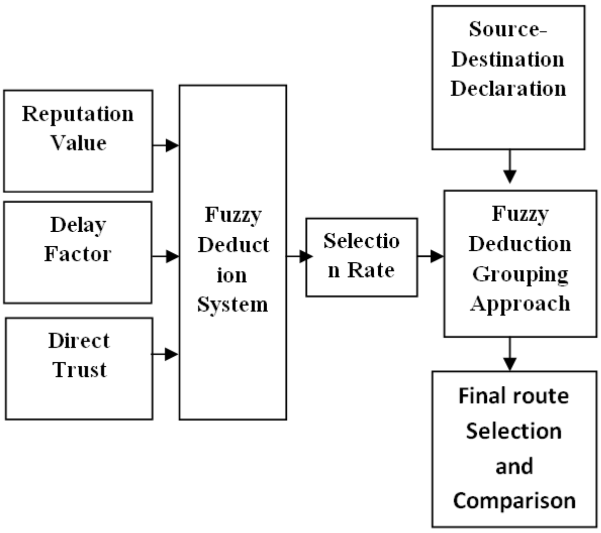

Reputation Value
Delay Factor
Direct Trust
Fuzzy Deduction System
Selection Rate
Source-Destination Declaration
Fuzzy Deduction Grouping Approach
Final route Selection and Comparison

Fig.2. Overview of the Fuzzy Deduction System (FDS) and node grouping approach

We have used Fuzzy Deduction System to compute the output of the given FDS inputs. This will gives the maximum selection rate of the nodes. For these six steps has to be followed:

1. Determining a set of fuzzy rules.
2. Fuzzifying the inputs using the input membership functions.
3. Combining the fuzzified inputs according to the fuzzy rules to establish rule strength (Fuzzy Operations).
4. Finding the consequence of the rule by combining the rule strength and the output membership function (implication).
5. Combining the consequences to get an output distribution (aggregation).
6. Defuzzifying the output distribution (this step is only if a crisp output (class) is needed).

After this, we have used Fuzzy deduction grouping algorithm to group the nodes to find out the node having maximum selection rate in each individual group. Selected node will be used for transmission of the data. Before vehicles and RSUs initialize a conversation with each other, four phases need to be performed during the revocation validation.

1. **Clustering**. In this part, vehicles and RSUs pre-process the latest CRL file using the two recently adjoin attributes, issued date and credibility, combined with both the **FDS**s clustering algorithm and the improved initial centroids choosing scheme in order to productively cluster the revocation certificates entries. A sampler visual of the clustering results is shown in Fig 3.
2. **Retrieving**. Upon receiving a connection set up request message from other vehicles, receivers will restrain the certificates contained in that message and educe all related data included in that certificate, that is, serial number, issue time, and credibility.
3. **Localizing**. Using the credibility and issued date, we can calculate the Euclidean Distance between the data point (i.e., new certificate) and all centroids in order to locate the closest cluster to join.
4. **Verifying**. In this part, the new data points that abut will check all neighboring data points in the latest joined cluster for a match in terms of credibility and issue date. If a match is found, this shows that its certificate has been revoked. Else, this data point is not in the CRL and can therefore be trusted.

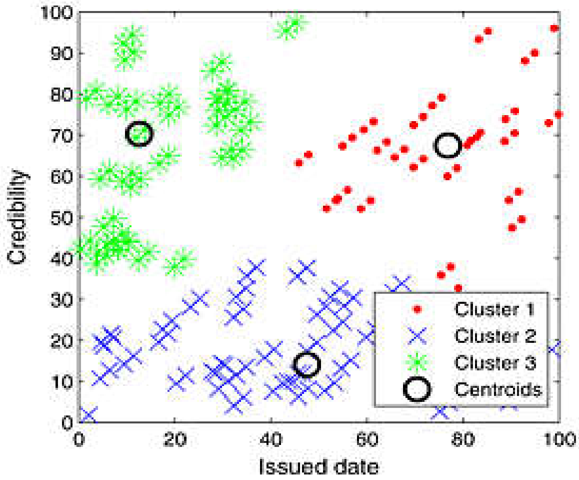


Fig.3. An example of clustering results using all entries in a CRL file, where n = 100, k = 3

For selecting the node for data transmission having maximum selection rate, Algorithm is given below: FDSs is an unsupervised knowledge forming and partitioning algorithm used for clustering n data points into k discrete clusters C, where the cluster Cj contains nj data points. Each cluster has a centroid, which represents a central vector used to assign different entities to that specific cluster. FDSs picks an initial centroid randomly, then uses Equation (1) to determine the next cluster centroids:

$$L = \sum_{j=1}^{k}\sum_{i=1}^{n}\left\| x_i - \mu_j \right\|^2 \qquad (1)$$

where xi is a vector denoting the xith data point, µj is the centroid of data points in Cj, and L is the distance for each data points to all centroids.

FDSs clustering algorithm is given below :

Algorithm 1 FDS Clustering Algorithm

```
Require: Input the number k of cluster centroids.
Ensure: Output k cluster.
1: Get $k$ = number of clusters.
2. Get $X = (x_1, x_2, \ldots, x_3), x_i \in R^d$
3. for $j = 1$ to $k$ do
4.     select $\mu_1, \mu_2, \ldots, \mu_k$ randomly
5. end for
6. for j=1 to k do
7.     for i=1 to n do
8.  determine
Repeat for K = 1 to N – 1  Begin
Repeat for J = 1 to N – K Begin
If ( A [ J ] < A [ J – 1 ] )
Swap ( A [ J ] , A [ J – 1 ] )
end for
end for
9.   end for
10. end for
11. Assign $x_i$ to $\mu_j$
12. After all data points have been assigned, recalculate the position of the centroids.
13. Repeat step 6 to 10 untill all centroids are convergent.
```

The centroids are considered as foregathered if their positions do not alter after a number of iterations. The algorithm can be discontinuing once the tth iteration has been achieved with an earliest given threshold of ϵ initially and those positions have been attested by the following inequality Equation (2):

$$\left| \frac{c^{t} - c^{t-1}}{c^{t}} \right| < \in \qquad (2)$$

where ct $^{-1}$ and ct are the previous and current locations of the centroid, respectively; t denotes the iteration; and ϵ is a given, pre-defined threshold.

RESULTS AND PERFORMANCE EVALUATION

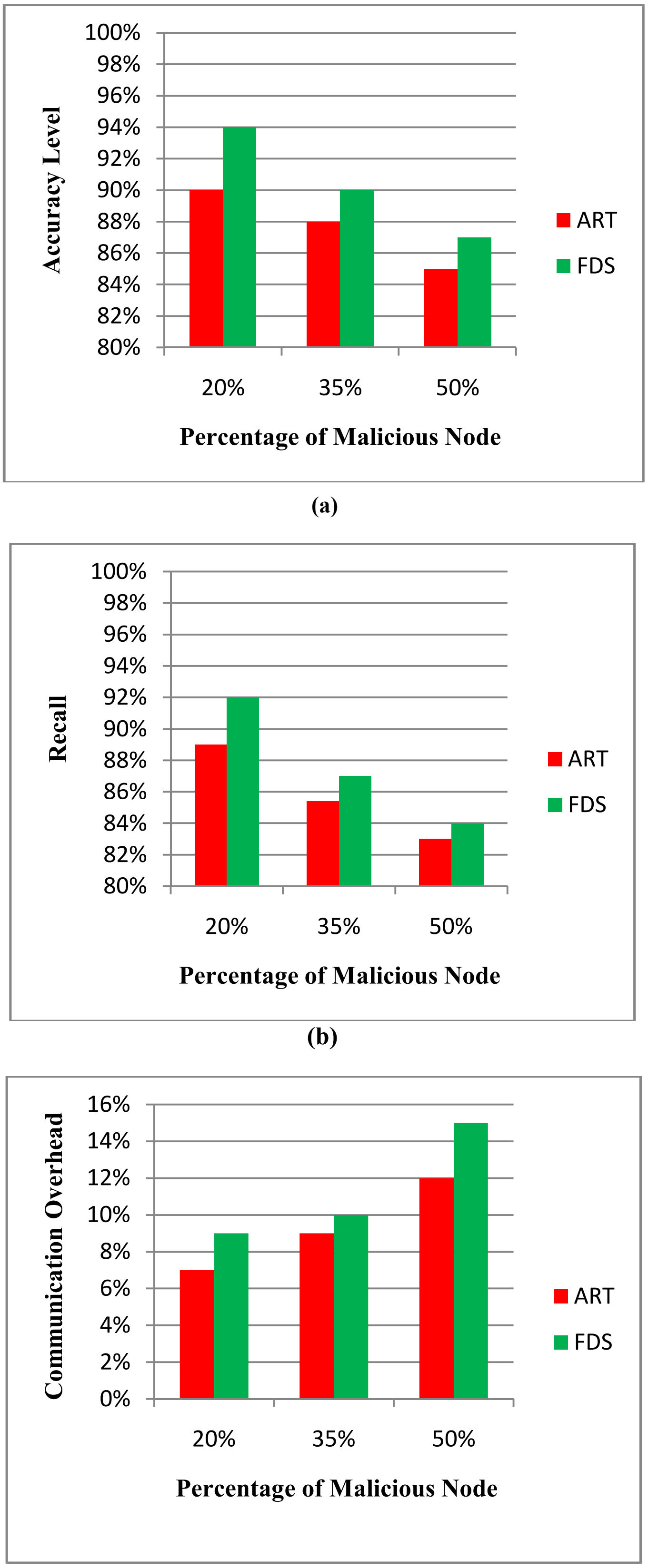
Table 1. Simulation Parameters

Parameter	Value
Simulation area	1000m × 1000m
Number of nodes	100, 200, 300
Transmission Range	150m
Node Placement	Random
Number of malicious node	10, 20, 30, 40
Simulation time	900s

In this section, the performance of the proposed ART scheme using fuzzy oriented intelligent system is evaluated and the experimental results are presented We use GloMoSim 2.03 as the simulation platform, and Table I lists the parameters used in the simulation scenarios. We use the ART scheme as the Baseline method. We have used the following two parameters to evaluate the accuracy of the ART scheme: Precision (P) and Recall (R), which are both widely used in intelligence system, machine learning and information retrieval to assess the accuracy (Davis and Goadrich, 2006). In this paper, we use both P and R values to evaluate how accurate the proposed Fuzzy system scheme is when it is used to identify untrustworthy nodes in VANETs. These two parameters are defined as follows.

$$P = \frac{\text{Num of Truly Malicious Nodes Caught}}{\text{Total Number of Untrustwo rthy Nodes Caught}}$$

$$R = \frac{\text{Number of Truly Malicious Nodes Caught}}{\text{Total Num of Truly Malicious Nodes}}$$



(a)

(b)

(c)

Fig 4. Effect of adversary percentage on ART and Fuzzy Deduction System. (a) Precision of FDS vs. ART. (b) Recall of FDS vs ART. (c) Communication Overhead of FDS vs ART

Fig. 4(a) shows the accuracy level for the ART scheme and for the fuzzy intelligent system with different percentages of malicious nodes. We find that accuracy level decrease when there are a higher percentage of malicious nodes, which is pretty obvious. In addition, the fuzzy oriented intelligent system is able to produce a better performance than the manual decision making method of ART scheme in terms accuracy level. Recall values in fig 4(b) also shows that Fuzzy System is again giving better performance than ART approach. In terms of communication overhead, Fig. 4(c) shows that the Fuzzy oriented system incur extra communication overhead compared to the ART when the percentage of malicious nodes varies.

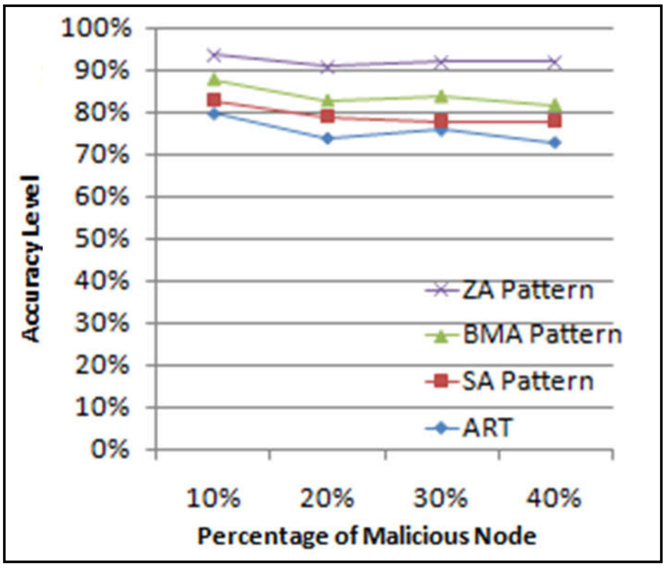


Fig. 5. Accuracy level of ART vs. SA, BMA, and ZA Pattern under fuzzy deduction system

In addition to this, we are also interested in knowing that how the fuzzy oriented intelligent system is resistant to different attack patterns, such as SA, BMA, and ZA. We also conducted some other experiments for fuzzy system, showing different types of malicious attacks and analyzing the performance of ART scheme with these attack patterns using fuzzy deduction system. The experiment results are in fig 5. From fig 5, we can clearly find the difference between traditional ART scheme and various attack patterns using fuzzy system. It can clearly identified that compared to traditional decision making approach, the fuzzy oriented deduction system is better resistant to various attack patterns as well as to the high percentage of malicious nodes in the network.

Conclusion and future work

In this research paper, the manual decision making process of attack resistant trust management scheme is replaced with prediction based artificial intelligence system i.e. fuzzy deduction system to evaluate the selection rate of individual node in the network. With this, FDS grouping approach is proposed to reduce the error rate in selecting the relay node. This also deals with different types of malicious attack and also estimates the trustworthiness data as well as nodes in vehicular adhoc networks.

To secure the data plane of vanets, trust management system was proposed. But the issues were that the model is only considering the factors trust which is calculated to its predicted value not on the present state QOS parameters. So there is need to propose a model which will analyze the system node and predict the trust of network to select the next hop for data transmission. A new algorithm is to be proposed that will consider sufficient and reliable list of parameters for high security purpose. It will add the present nodes quality parameters and help in predicting the trust of the nodes. This will helps in making data plane more secure and trust worthy.

REFERENCES

Daeinabi, A. and Rahbar, A.G. 2013. Detection of malicious vehicles (DMV) through monitoring in vehicular ad-hoc networks. *Multimedia Tools Appl*. 66(2), 325–338.

Davis J. and M. Goadrich, 2006. “The relationship between precision–recall and ROC curves,” in *Proc. ACM 23rd Int. Conf. Mach. Learn.*, pp. 233–240.

Engoulou, R. G., Bellache, M., Pierre, S. and A. Quintero. 2014. VANET security surveys,” *Comput. Commun.*, vol. 44, pp. 1–13.

Gerlach, M. 2006. Full paper*:* assessing and improving privacy in *VANETs*. www.network-on-wheels.de/down loads /escar2006gerlach.pdf (accessed: May 29, 2010).

Ghosh, M., Varghese, A., Gupta, A., Kherani, A.A. and Muthaiah, S.N. 2010. Detecting misbehaviors in VANET with integrated root-cause analysis. Ad Hoc Netw. 8, 778–790.

Ghosh, M.,Varghese,A., Kherani,A.A. and Gupta, A. 2009. Distributed misbehavior detection inVANETs. In: Wireless Communications and Networking Conference,WCNC IEEE, pp. 1–6.

Harsch, C., Festag, A. and Papadimitratos, P. 2007. Secure position-based routing for VANETs. In *Proceedings of IEEE 66th vehicular technology conference (VTC-2007), Fall,* (pp. 26–30).

Kadam, M., Limkar, S. D. and PMV. 2014. new approach for detection and prevention of misbehave/malicious vehicles from VANET. In: Proceedings of the International Conferenceon Frontiers of Intelligent Computing: Theory and Applications (FICTA) 2013. AISC, vol. 247, pp. 287–295. Springer, Heidelberg.

Kim, C.H. and Bae, I.H. 2012. A misbehavior based reputation management system for VANETS. LNEE 181, 441–450.

Li, W. and H. Song, 2015. “ART: An Attack-Resistant Trust Management Scheme for Securing Vehicular Ad Hoc Networks,”*IEEE.*

Lin Y. and H. Song, 2006. “DynaCHINA: Real-time traffic estimation and prediction,” *IEEE PervasiveComput.*, vol. 5, no. 4, pp. 65–65.

Raya, M., and Hubaux, J. 2005. The security of vehicular ad hoc networks. In *Proceedings of the 3rd ACM workshop on security of ad hoc and sensor networks (SASN 2005)* (pp.1–11), Alexandria, VA.

Wahab, O.A., Otrok, H. and Mourad, A. 2014. A cooperative watchdog model based on Dempster- Shafer for detecting misbehaving vehicles. Comput. Commun. 41, 43–54 *Elsevier.*

****