ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 1, February 2017

Misbehavior Detection in Vanet using an attack Resistant trust management scheme

D.Maheswari, S.Sekar & V.Manju Barkavi
M.Tech-Information and cyber warfare, dept. of IT
Kongu Engineering College
Perundurai, India
dmaheswaridivi@gmail.com

Dr. G.K.Kamalam
Assistant Professor, dept. of IT
Kongu Engineering College
Perundurai, India
gkk@kongu.ac.in

***Abstract*—Vehicular ad hoc networks (VANETs) have the potential to transform the way in which the people can travel through the creation of a safe interoperable wireless communication networks (cars, buses, traffic signals, cell phones, and other devices). In Base Line Weighted Voting (BLWV) method, it calculates only the trust value on each node by separate weight calculation of nodes. The proposed Attack-Resistant Trust Management (ART) scheme evaluates the trustworthiness of traffic data and vehicle nodes in VANETs and also easily detects the various malicious attacks. In ART scheme, Dumpster's rule is applied to combine the local evidences collected by a mobile node and from the other external mobile nodes. The trustworthiness of data and nodes are evaluated into two separate metrics, Data trust and Node trust. The data trust is used to assess the traffic data and also reports in what extend the traffic data are trustworthy and the node trust indicates how the nodes are trustworthy. The trust management theme is applicable to a wide range of VANET applications in order to improve the traffic safety, mobility, and environmental protection. The effectiveness and efficiency of the ART scheme is validated through extensive experiments. This scheme accurately evaluates the trustworthiness of data and the nodes in VANETs.**

Keywords*—VANETs; trust management; security; misbehavior detection

I. INTRODUCTION

In recent years, the growing needs for increased safety and efficiency of road transportation system have promoted automobile manufacturers to integrate wireless communications and networking into vehicles. The wirelessly networked vehicles naturally form Vehicular Ad-hoc Networks (VANETs), in which vehicles cooperate to relay various data messages through multi-hop paths, without the need of centralized administration. VANETs have the potential to transform the way people travel through the creation of a safe, interoperable wireless communications network.

In VANETs, various nodes, such as vehicles and Roadside Units (RSUs), are generally equipped with sensing, processing, and wireless communication capabilities. Both Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communications enable safety applications that provide warnings regarding road accidents, traffic conditions (e.g., congestion, emergency braking, icy road) and other relevant transportation events. However, VANETs are vulnerable to threats due to increasing reliance on communication, computing and control technologies. The unique security and privacy challenges posed by VANETs include integrity (data trust), confidentiality, nonrepudiation, access control, real-time operational constraints/demands, availability, and privacy protection.

II. RELATED WORK

In recent years, there has been significant research interest in the topics of misbehavior detection as well as trust management for ad hoc networks.

A. Misbehavior Detection for Ad hoc Networks

First, Note that the term *misbehavior* generally refers to abnormal behavior that deviates from the set of behaviors that each node is supposed to conduct in ad hoc networks [12]. According to [13], there are four types of misbehaviors in ad hoc networks, namely failed node behaviors, badly failed node behaviors, selfish attacks, and malicious attacks. These four types of node misbehaviors are classified with respect to the node's intent and action. More specifically, selfish attacks are intentional passive misbehaviors, where nodes choose not to fully participate in the packet forwarding functionality to conserve their resources, such as battery power; malicious attacks are intentional active misbehaviors, where the malicious node aims to purposely interrupt network operations. The existence of selfishness and malicious behaviors has remarkably motivated research in the area of misbehavior detection for mobile ad hoc networks (MANETs).

Alternatively, there have been some attacks which primarily focus on the data that are transmitted and shared

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 1, February 2017

among nodes in ad hoc networks. Thus, another goal of misbehavior detection approaches is to ensure that data has not been modified in transit, that is, they should make sure that what was sent is the same as what was received. More specifically, some of the widely-studied data trust attacks are masquerading attack, replay attack, message tampering attack, hidden vehicle attack, and illusion attack [10]–[12].

Intrusion Detection System (IDS) is normally regarded as an important solution for detecting various node misbehaviors in ad hoc networks. Several approaches have been proposed to build IDS probes on each individual peer due to the lack of a fixed infrastructure, such as [8]–[9]. In these approaches, there is one IDS probe installed on each node, and each IDS probe is assumed to be always monitoring the network traffic, which is obviously not energy efficient given the limited battery power that each node has in MANETs. In contrast, Huang *et al.* [2] proposed a cooperative intrusion detection framework in which clusters are formed and the nodes in each cluster fulfill the intrusion detection task in turn. This cluster-based approach can noticeably reduce the power consumption for each node. Christo Ananth et al. [7] discussed about a system, In this proposal, a neural network approach is proposed for energy conservation routing in a wireless sensor network. Our designed neural network system has been successfully applied to our scheme of energy conservation. Neural network is applied to predict Most Significant Node and selecting the Group Head amongst the association of sensor nodes in the network. After having a precise prediction about Most Significant Node, we would like to expand our approach in future to different WSN power management techniques and observe the results. In this proposal, we used arbitrary data for our experiment purpose; it is also expected to generate a real time data for the experiment in future and also by using adhoc networks the energy level of the node can be maximized. The selection of Group Head is proposed using neural network with feed forward learning method. And the neural network found able to select a node amongst competing nodes as Group Head. There are also some other solutions that aim to cope with various routing misbehaviors [2]–[4].

B. Trust Establishment and Management in Ad hoc Networks

The main purpose of trust management is to assess various behaviors of other nodes and build a reputation for each node based on the behavior assessment. The reputation can be utilized to determine trustworthiness for other nodes, make choices on which nodes to cooperate with, and even take action to punish an untrustworthy node if necessary. In general, the trust management system usually relies on two sorts of observations to evaluate the node behaviors. The first kind of observation is named as *first-hand* observation, or in other words, direct observation [5]. First-hand observation is the observation that is directly made by the node itself, and the first-hand observation can be collected either passively or actively. If a node promiscuously observes its neighbors' actions, the local information is collected passively. In contrast, the reputation management system can also rely on some explicit evidences to assess the neighbor behaviors, such as an acknowledgement packet during the route discovery process. The other kind of observation is called *second-hand* observation or indirect observation. Second-hand observation is generally obtained by exchanging first-hand observations with other nodes in the network. The main disadvantages of second-hand observations are related to overhead, false report and collusion [6].

In [8], Buchegger *et al.* proposed a protocol, namely CONFIDANT (Cooperation of Nodes, Fairness in Dynamic Ad-hoc NeTworks), to encourage the node cooperation and punish misbehaving nodes. CONFIDANT has four components in each node: a Monitor, a Reputation System, a Trust Manager, and a Path Manager. The Monitor is used to observe and identify abnormal routing behaviors. The Reputation System calculates the reputation for each node in accordance with its observed behaviors. The Trust Manager Exchanges alerts template is used to format your paper and style the text. All margins, column widths, line spaces, and text fonts are prescribed; please do not alter them. You may note peculiarities. For example, the head margin in this template measures proportionately more than is customary. This measurement and others are deliberate, using specifications that anticipate your paper as one part of the entire proceedings, and not as an independent document. Please do not revise any of the current designations with other trust managers regarding node misbehaviors. The Path Manager maintains path rankings, and properly responses to various routing messages. A possible drawback of CONFIDANT is that an attacker may intentionally spread false alerts to other nodes that a node is misbehaving while it is actually a well-behaved node. Therefore, it is important for a node in CONFIDANT to validate an alert it receives before it accepts the alert.

Michiardi *et al.* [9] presented a mechanism called CORE to identify selfish nodes, and then compel them to cooperate in the following routing activities. Similar to CONFIDANT, CORE uses both a surveillance system and a reputation system to observe and evaluate node behaviors. Nevertheless, while CONFIDANT allows nodes exchange both positive and negative observations of their neighbors, only positive observations are exchanged amongst the nodes in CORE. In this way, malicious nodes cannot spread fake charges to frame the well-behaved nodes, and consequently avoid denial of service (DoS) attacks toward the well-behaved nodes. The reputation system maintains reputations for each node, and the reputations are adjusted upon receiving of new evidences. Since selfish nodes reject to cooperate in some cases, their

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 1, February 2017

reputations are lower than other nodes. To encourage node cooperation and punish selfishness, if a node with low reputation sends a routing request, then the request will be ignored and the bad reputation node cannot use the network.

Patwardhan *et al.* [3] studied an approach in which the reputation of a node is determined by data validation. In this approach, a few nodes, which are named as Anchor nodes here, are assumed to be pre-authenticated, and thus the data they provide are regarded as trustworthy. Data can be validated by either agreement among peers or direct communication with an anchor node. Malicious node can be identified if the data they present is invalidated by the validation algorithm.

III. PROPOSED METHOD

In this section, the research problem that is addressed in this paper will be described in more details, including the network model as well as the adversary model.

A. *Network Model*

A VANET generally refers to a wireless network of heterogeneous sensors or other computing devices that are deployed in vehicles. This type of network enables continuous monitoring and sharing of road conditions 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.

B. *Adversary Model*

First of all, the RSUs are assumed to be trustworthy since they are usually better protected. The connected vehicles, on the other hand, are generally more susceptible to various attacks, and they can be compromised at any time after the VANET is formed.

The adversary 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 adversary is able to eavesdrop, jam, modify, forge, or drop the wireless communication between any devices in range. The main goals of the adversary 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.

1. Simple attack
2. Bad Mouth Attack
3. Zigzag Attack

1) Simple Attack

An attacker may manipulate the compromised nodes not to follow normal network protocols and not to provide necessary services for other nodes, such as forwarding data packets or propagating route discovery requests. However, the compromised node will not provide any fake trust opinions when it is asked about other node's trustworthiness.

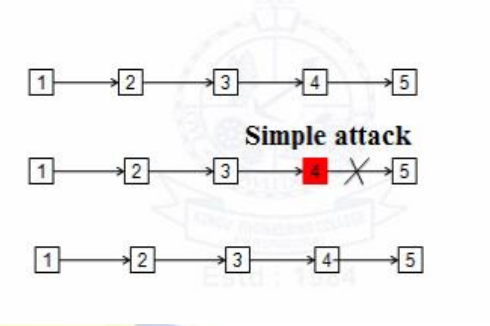

Figure 1.Simple Attack

2) Bad Mouth Attack

In addition to conduct simple attack, the attacker can also spread fake trust opinions and try to frame the benign nodes so that the truly malicious nodes can remain undetected. This attack aims to disrupt the accurate trust evaluation and make it harder to successfully identify the malicious attackers.

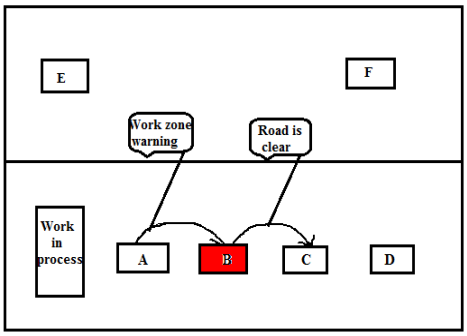

Figure 2.Bad Mouth Attack

3) Zigzag Attack

Sometimes sly attackers can alter their malicious behavior patterns so that it is even harder for the trust management scheme to detect them. For instance, they can conduct malicious behaviors for some time and then stop for a while (in that case the malicious behaviors are conducted in an on-and-off manner). In addition, the sly attackers can also exhibit different behaviors to different audiences, which can lead to inconsistent trust opinions to the same node among different audiences. Due to the insufficient evidence to accuse the

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 1, February 2017

malicious attacker, it is generally more difficult to identify such sly attackers.

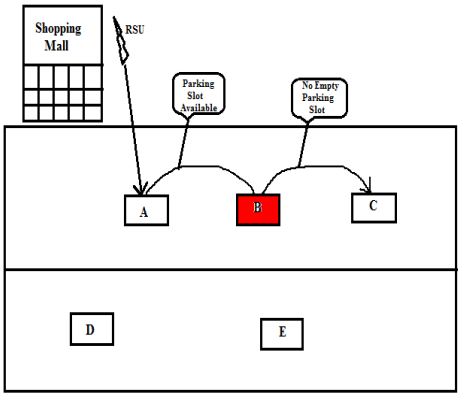

Figure 3.Zigzag Attack

C. Art Schema for Securing Vanet

In this section, the proposed ART scheme is presented in details. The ART scheme addresses two types of trustworthiness in VANETs: *data trust* and *node trust*.

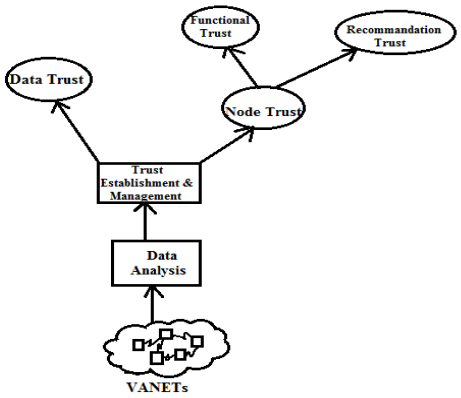

Figure 4.Overview of the ART scheme

1) Evidence Combination

Evidence combination is very important for the ART scheme. Because in some of the traffic data may not reliable, so it is critical to find an evidence combination technique to properly fuse together the multiple pieces of evidence in both trustworthy and untrustworthy data. It is necessary to combine multiple pieces of evidences so that data trust and functional trust can be evaluated using Dempster–Shafer Theory of evidence (DST). Then it combines the local evidences collected by a mobile node and the external evidences shared by other mobile nodes.

2) Evaluation of Trust Recommendations Using Collaborative Filtering

In VANET, it is not feasible for two different vehicle nodes to communicate directly with each other. In this case, it is essential for one vehicle node to relay data for others. Sometimes a node may refuse to relay data because of its limited battery power or other resources, or the node may have been compromised by adversaries. It is critical to know vehicle is trustworthy to interact with or not if a vehicle has never interacted with others before, then the trust recommendations receives data from others. Then only that data can rely on to evaluate the trustworthiness of other nodes.

Nodes which have similar trust preferences on some nodes may also have similar preferences. Thus, this method provides recommendations or predictions over target node based on the opinions of other like-minded nodes. The recommendation trust is determined using the following steps.

- Trust rating formation
- Trusted neighbor selection
- Predicted trust calculation

a) *Trust rating formation*

Trust rate of two nodes are denoted by cosine of angle between dot product of two vectors. If a node evaluates a node, then default rating is used.

$$\cos(\vec{i},\vec{j}) = \frac{\vec{i} \bullet \vec{j}}{\| \vec{i} \| * \| \vec{j} \|}$$

b) Trusted Neighbor Selection

Similarities between nodes in the model are computed and the top most similar nodes are selected. The functional trust of each selected node will also be inspected to make sure those only recommendations from the nodes which can fulfill the tasks as expected will be trusted.

$$\text{Neighbor node} = \sqrt{(x_1 - x_2)^2 + (y_1 - y_2)^2}$$

c) *Predicted Trust Calculation*

Predicted trust rating of node i on node k calculated by this formula,

$$T_{ik} = \bar{R}_i + \frac{\sum_{j \in s_i} \cos(i, j) * (R_{j,k} - \bar{R}_j)}{\sum_{j \in s_i} |\cos(i, j)|}$$

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 1, February 2017

IV. RESULT ANALYSIS

ART scheme is evaluated by the precision and recall. Precision and recall values are used to evaluate how accurate the proposed ART scheme. It is used to identify the untrustworthy of nodes in VANETs.

$$P = \frac{\text{Num of Truly Malicious Nodes Caught}}{\text{Total Num of Untrustworthy Nodes Caught}}$$

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

Simple Attack

The figure 5 represents the precision and recall values of simple attack.

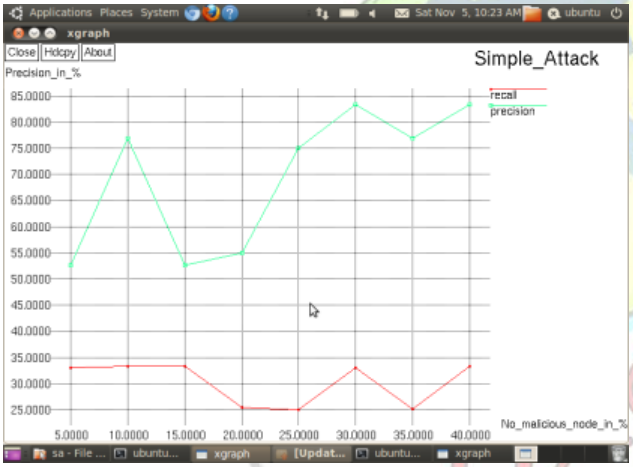

Figure 5.Precision and Recall for Simple attack

Bad Mouth Attack

The figure 6 represents the precision and recall values of bad mouth attack.

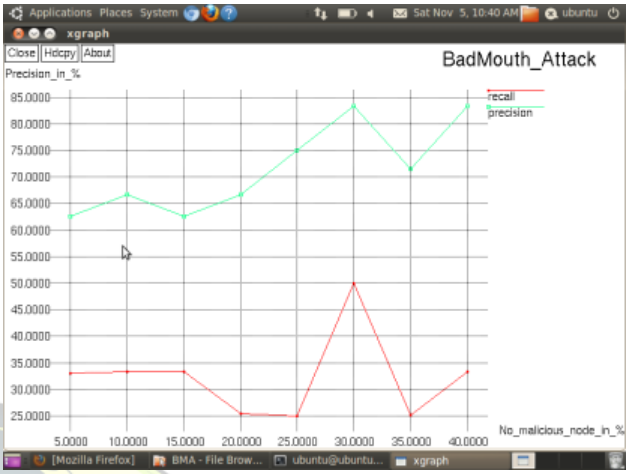

Figure 6.Precision and Recall for Bad Mouth attack

Zigzag Attack

The figure 7 represents the precision and recall values of zigzag attack

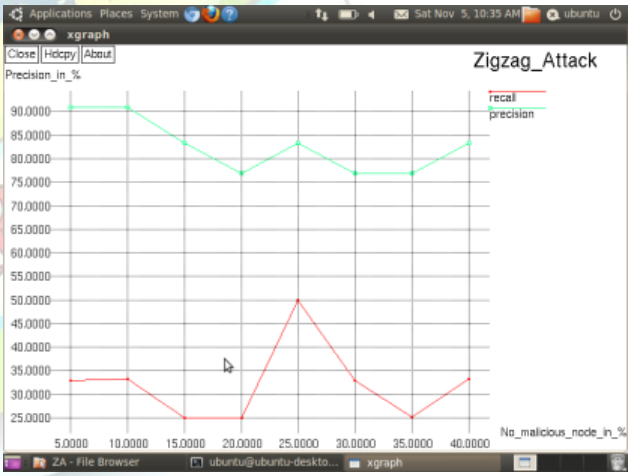

Figure 7.Precision and Recall for Bad Mouth attack

V.CONCLUSION

An attack-resistant trust management scheme is to evaluate the trustworthiness in traffic data and the vehicle nodes in VANETs. In the ART scheme, the trustworthiness of the data and the nodes are evaluated into two separate metrics as Data trust and Node trust. The data trust is used to assess the traffic data and also reports in what extend the traffic data are trustworthy. The node trust indicates how the nodes are trustworthy. To validate the trust management scheme an

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 1, February 2017

extensive experiments have been conducted and the experimental results are shown. So the proposed ART scheme evaluates the trustworthiness of data and the nodes in VANETs. Using this scheme it can cope with various malicious attacks. In future, the proposed schema is based on Sybil attack because the attacker sends multiple messages to other vehicles. Each message may contain different source identity. The main aim of the attacker is to provide an illusion of multiple vehicles to other vehicles so that vehicles can choose another route.

References

[1] Adomavicius G and Tuzhilin A (2005), "Toward the Next Generation of Recommender Systems: A survey of the State-of-the-Art and Possible Extensions", IEEE Transactions on Knowledge and Data Engineering, Vol. 17, No. 6, pp. 734–749.

[2] Buchegger S and Le Boudec J Y (2002), "Performance Analysis of the Confidant Protocol", Journal of Future Generation Computer Systems, pp. 226–236.

[3] Chen I-R, Bao F, Chang M, and Cho J-H (2014), "Dynamic Trust Management for Delay Tolerant Networks and its Application to Secure Routing", IEEE Transactions on Parallel Distribution System, Vol. 25, No. 5, pp. 1200–1210.

[4] Engoulou R G, Bellache M, Pierre S, and Quintero A (2014), "VANET Security Surveys", Journal of Computer Communications, Vol. 44, pp. 1–13.

[5] He Q, Wu D, and Khosla P (2004), "SORI: A Secure and Objective Reputation based Incentive Scheme for Ad-hoc Networks", in proceedings of IEEE WCNC, Vol. 2, pp. 825–830.

[6] Hu Y-C, Perrig A, and Johnson D B (2002), "Ariadne: A Secure On-Demand Routing Protocol for Ad-hoc Networks", Journal of Mobile Computing and Networks, pp. 12–23.

[7] Christo Ananth, A.Nasrin Banu, M.Manju, S.Nilofer, S.Mageshwari, A.Peratchi Selvi, "Efficient Energy Management Routing in WSN", International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE), Volume 1, Issue 1, August 2015,pp:16-19

[8] Lu R, Lin X, Liang X, and Shen X (2012), "A Dynamic Privacy-Preserving Key Management Scheme for Location-Based Services in VANETs", IEEE Transactions on Intelligent Transportation Systems, Vol. 13, No. 1, pp. 127–139.

[9] hMejri M N, Ben-Othman J, and Hamdi M (2014), "Survey on VANET Security Challenges and Possible Cryptographic Solutions", Journal of Vehicular Communications, Vol. 1, No. 2, pp. 53–66.

[10] Raya M, Papadimitratos P, Gligor V D, and Hubaux J P (2008), "On Data Centric Trust Establishment in Ephemeral Ad-hoc Networks", in proceedings of IEEE INFOCOM, pp. 1238–1246.

[11] Sharef B T, Alsaqour R A, and Ismail M (2014), "Vehicular Communication Ad hoc Routing Protocols: A survey", Journal of Network Computation and Applications, Vol. 40, pp. 363–396.

[12] Taha S and Shen X (2013), "A Physical-Layer Location Privacy-Preserving Scheme for Mobile Public Hotspots in NEMO-based VANETs", IEEE Transactions on Intelligent Transportation Systems, Vol. 14, No.4, pp.1665–1680.