# A Misbehavior Detection System for Vehicular Delay Tolerant Networks

Yinghui Guo, Sebastian Schildt, Johannes Morgenroth, Lars Wolf

IBR, Technische Universität Braunschweig
Mühlenpfordstraße 23, 38106, Braunschweig, Germany
{ guo | schildt | morgenro | wolf }@ibr.cs.tu-bs.de

**Abstract:** In vehicular networks, many vehicles participate in the network and transfer messages for each other. At least for the next years, i.e., until a high rate of vehicles equipped with according network technology has been reached, we believe that delay-tolerant methods are useful in such networks, leading to Vehicular Delay Tolerant Networks. However, in such a cooperative system malicious or selfish nodes may exist which can have a devastating effect on network performance. Traditional security protocols cannot completely address such problems in Vehicular Delay Tolerant Networks. Hence we propose a misbehavior detection system to defend against these attacks. By collecting and securely exchanging data of previous encounters, vehicles can assess the trustworthiness of other vehicles in order to detect malicious nodes. We present preliminary simulation results showing that our misbehavior detection system performs effectively.

## 1 Introduction

In Vehicular Ad Hoc Networks (VANETs), a vehicle is equipped with short-range radios and computing resources and has the ability to communicate with fixed roadside infrastructure or other nearby vehicles. However, due to the high movement of vehicles, the connectivity in VANETs is highly unstable and links may change or break soon after they have been established. Delay- and Disruption-Tolerant Networking (DTN) is designed to operate under such conditions. DTN implements a 'store, carry and forward' paradigm [D09]. A packet will be sent over an existing link and buffered at the next hop until a connection to a suitable next hop is established. Several projects using Vehicular Delay Tolerant Networks (VDTNs) exist: By using buses, motorcycles or even bicycles DakNet,[1] developed by MIT Media Lab researchers, provides digital connectivity to outlying villages in India lacking a digital communications infrastructure. In Optracom,[2] developed by IBR researchers, the public transport system composed of buses and trams is used to gather air pollution measurements.

[1] http://www.firstmilesolutions.com/
[2] http://www.ibr.cs.tu-bs.de/projects/optracom/

Common vehicular networks typically assume cooperation and no malicious behavior from all participating vehicles. However, vehicles are individual entities that can make independent decisions regarding the forwarding or deletion of messages. Some of the vehicles may be malicious, trying their best to destroy or disrupt the network. Therefore security considerations are clearly an important issue. Some work has focused on authentication and encryption, such as [AKGOL07]. Even though authentication and encryption are efficient methods to defend the system against outside attackers, it cannot safeguard the system from inside attackers. Hence a flexible Misbehavior Detection System (MDS) is essential for VDTNs.

For our MDS we propose a general mechanism to detect spurious information and identify the behavior of the nodes. By collecting information by themselves or sharing with immediate neighbors, our MDS can ultimately identify a culprit after an attack and prevent the network from being impaired again.

The remainder of this paper is structured as follows. Section 2 discusses related work. Section 3 introduces the attack and the vehicular network model. In Section 4, we explain our architecture and detection scheme. The simulation-based evaluation is presented in Section 5. Finally, in Section 6 we draw our conclusions and describe future work.

## 2 Related work

Much work has been done in the area of MDS to detect or mitigate the effects of malicious nodes. In ad hoc networks, by eavesdropping on neighbors [MGLB00] uses a watchdog and pathrater to detect and mitigate routing misbehavior. [BB02] presents a MDS called CONFIDANT, which is composed of Monitor, Trust Manager, Reputation System and Path Manager. This system not only detects malicious nodes but also punishes them. However, due to the lack of long-lasting links in VDTNs, it is impractical to continuously monitor neighbors for detection.

In the MDS presented in [RPAJH07], once a vehicle detects another misbehaving vehicle, a warning is triggered and sent out to other vehicles. To prevent wrong accusations, the LEAVE protocol is designed for summing warnings and dealing with accusations. Only when a vehicle exceeds the defined threshold of LEAVE, disregard messages are triggered and sent out to Certification Authority (CA). Although LEAVE can detect malicious vehicles, it needs a CA as the central component.

The MDS in [RCYC10] proposes encounter tickets. When two nodes meet, after transmitting data, they also create a ticket about this encounter. When the node encounters other nodes, these tickets will be exchanged and used to detect blackholes. A similar system is presented in [LC12]. Based on the contact records, a node can detect if other nodes drop packets. To prevent collusion of attackers, the contacted node also randomly asks witness nodes for help. Nevertheless, these MDS only focus on blackhole attacks while our MDS is designed to not only detect blackholes, but also deal with selfish nodes. And compared to [LC12], our MDS can independently detect evil nodes.

# 3 System model

## 3.1 Attack model

In VDTNs, a node may agree to forward packets but actually drop them, because it is selfish or malicious. Considering energy and memory, selfish nodes may be reluctant to cooperate if it is not directly beneficial to them. Therefore, selfish nodes will be given incentive to encourage them to forward others' messages. Malicious nodes try to disrupt the network. The most common attack is the blackhole attack. Blackholes may advertise many excellent routes through themselves and then drop all of the packages [CY06].

## 3.2 Vehicular network model

Our VDTN is composed of Roadside Units (RSUs) and vehicles, each possessing their own private and public key pair and unique identifier. The network is loosely time synchronized, RSUs and vehicles will be in the same time slot at any time.

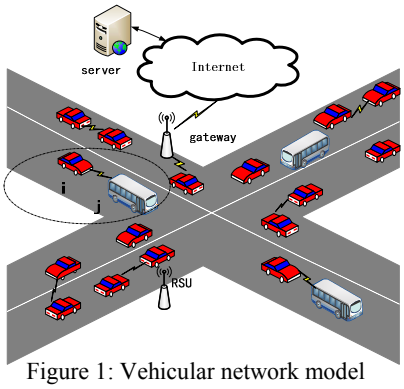


Figure 1: Vehicular network model

RSUs can work as a gateway, possibly transmitting information to the Internet. Besides, RSUs are also responsible for collecting reports from vehicles and make an appropriate decision to deal with attackers. Each vehicle runs its own instance of the MDS to independently detect attackers and build its own local blacklist. Figure 1 shows the scenario in which vehicle i transmits messages to vehicle j in VDTNs.

# 4 System architecture

The system is composed of the observation module, the evaluation module and the decision module.

## 4.1 Observation module

In the observation module, RSUs and vehicles focus on generating Encounter Records (ERs). An ER will be generated after two vehicles met and successfully exchanged

messages. When a vehicle meets another vehicle, before transferring messages, it first needs to submit its ERs for verification. Here, we use vehicle i and j as an example to illustrate how the ER is constructed. Vehicle i generates ER for j as follows:

$$ER_i = ID_i, ID_j, sn_i, sn_j, t, \mathrm{Re}_{i\to j}, \mathrm{Re}_{j\to i}, sig_i, sig_j$$

$$\mathrm{Re}_{i\to j} = \{ (msg_{id}, msg_{src} \mid \ i\ send\ \ msg\ \ to\ \ j) \} \qquad \mathrm{Re}_{j\to i} = \{ (msg_{id}, msg_{src} \mid \ j\ send\ \ msg\ \ to\ i) \}$$

$$sig_i = E_{RK_i}\left\{H\left(ID_i \middle| ID_j \middle| sn_i \middle| sn_j \middle| t \middle| \mathrm{Re}_{i\to j} \middle| \mathrm{Re}_{j\to i}\right)\right\} \qquad sig_j = E_{RK_j}\left\{H\left(ID_i \middle| ID_j \middle| sn_i \middle| sn_j \middle| t \middle| \mathrm{Re}_{i\to j} \middle| \mathrm{Re}_{j\to i}\right)\right\}$$

The content of ER includes both of the vehicles' identifiers, $ID_i$ and $ID_j$. The unique sequence number $sn$ of each vehicle starts from 1 and is increased by one after each contact. A vehicle is not allowed to use the same $sn$ twice. $t$ shows the time when this ER was generated. The ERs in [LC12] use a vector of packets buffered by nodes, the identifiers of the packets received by nodes and the identifiers of the packets sent by nodes to detect blackholes. This will make the size of the record too large if there is sufficient traffic in the system. In our system we introduce the $\mathrm{Re}$ set, which identifies the transmitted messages. The $\mathrm{Re}_{i\to j}$ set consists of (id, src) 2-tuples storing for each message that has been received by j from i the message's id, and the id of the originating node. $\mathrm{Re}_{j\to i}$ contains the message information sent from vehicle j to i. Both vehicles sign the ER with their private keys for integrity protection. $E_{RK_i}\{*\}$ and $E_{RK_j}\{*\}$ denote the encryption using vehicle i and j's private key. Here we use $H(*)$ to denote a hash function, and | to denote the concatenation operation. It is not practical to provide all ERs when two vehicles meet. Therefore we define a short report window W, a vehicle only submits W new and sequential ERs to other vehicles. We choose W to be 5.

### 4.2 Evaluation module

In the evaluation module, vehicles measure the trustworthiness of other vehicles, called Trust Reputation (TR). When a vehicle first joins into the network, it has the same initial TR (defined as 0.5) for other vehicles. After receiving ERs from the observation module, TR will be updated. The range of TR is between 0 and 1. When vehicle i encounters j, the evaluation module will check the following conditions:

1) We assume each vehicle has its own local blacklist. When vehicle i adds vehicle j into its blacklist, it will simultaneously delete the TR and other relevant information of j. If vehicle j is in i's blacklist, j will be refused to transfer and receive message from i.

2) When two vehicles meet, both need to provide W new and sequential ERs to each other. If vehicle j behaves well, the $sn$ in its W ERs should be sequential. If vehicle j chooses better ERs from its memory to cheat others, the $sn$ will be not sequential anymore. Once i finds the $sn$ of j is not sequential, j will be added into i's local blacklist.

3) Vehicle i has a meeting list which records for all its encountered vehicles' $ID$, $sn$ and time. If vehicle i met j before, by checking $sn$ and $t$ from j's ERs and comparing with its

meeting list, vehicle i can prevent an advanced attacker from only providing old and good ERs or deleting ERs which are disadvantageous to itself. Once vehicle i detects these behaviors, it will add j into its local blacklist.

4) If vehicle j passes the checks 1 to 3, vehicle i will use the $\mathrm{Re}_{i\to j}$ and $\mathrm{Re}_{j\to i}$ sets to update the TR of j. Vehicle i first figures out the message forwarding ratio of j, which is the total number of messages that are sent out by j in W ERs over the total number of messages received by j. Vehicle j provides W ERs: $\mathrm{Re}_0$, $\mathrm{Re}_1$,.., $\mathrm{Re}_{W-1}$. $N_{send}^{\mathrm{Re}_0}$, $N_{send}^{\mathrm{Re}_1}$, …, $N_{send}^{\mathrm{Re}_{W-1}}$ show how many messages are sent out by j in ER 0,1, …W-1. $N_{recv}^{\mathrm{Re}_0}$, $N_{recv}^{\mathrm{Re}_1}$, …, $N_{recv}^{\mathrm{Re}_{W-1}}$ show how many messages are received by j in ER 0,1, …W-1. The message forwarding percentage $\theta$ can be expressed as formula (1).

$$\theta = \frac{\sum_{i=0}^{i<W} N_{send}^{\mathrm{Re}_i}}{\sum_{i=0}^{i<W} N_{recv}^{\mathrm{Re}_i}} \qquad (1)$$

If $\theta > N_{threshold}$, we can proceed to step 5. If $\theta \le N_{threshold}$ this indicates that vehicle j may selectively drop messages. The TR of j will be decreased according to formula (2).

$$TR_i^j = TR_i^j - \gamma \quad (0<\gamma<1) \qquad (2)$$

5) A blackhole drops all messages, so it only transmits the messages which are generated by it. The same applies to selfish nodes. To prevent this, we use another mechanism to find malicious vehicles. Again $N_{send}^{\mathrm{Re}_0}$, $N_{send}^{\mathrm{Re}_1}$, …, $N_{send}^{\mathrm{Re}_{W-1}}$ show how many messages are sent out by j in ER 0,1, …W-1. $N_{send}^{j\mathrm{Re}_0}$, $N_{send}^{j\mathrm{Re}_1}$, … $N_{send}^{j\mathrm{Re}_{W-1}}$ are the number of messages which j generates by itself and sends out in ER 0,1, …W-1. $\psi$ is defined as the vehicle's own message forwarding percentage, shown as formula (3).

$$\psi = \frac{\sum_{i=0}^{i<W} N_{send}^{j\,\mathrm{Re}_i}}{\sum_{i=0}^{i<W} N_{send}^{\mathrm{Re}_i}} \qquad (3)$$

If $\psi \ge NR_{threshold}$, it shows that vehicle j prefers to send its own messages. This kind of behavior will be punished. We use formula (2) to decrease TR. If step 4 and 5 simultaneously detect the bad behavior of vehicle j, we use formula (4) to finally decrease TR. If neither of them detects abnormal behavior, it shows that vehicle j is normal. Then vehicle j will be encouraged and the TR is updated according to formula (5). To encourage more vehicles to participate into the network, the additive component $\lambda$ is larger than the subtractive component $\gamma$. Only when vehicle i is convinced that vehicle j behaves badly, the larger subtractive component $\rho$ is applied to decrease the TR of j. In this paper we choose $\gamma$ to be 0.02, $\rho$ to be 0.05, $\lambda$ to be 0.03, $N_{threshold}$ to be 0.55, and $NR_{threshold}$ to be 0.7. The updated TR will be delivered to the decision module.

$$TR_i^j = TR_i^j - \rho \quad (0<\rho<1) \qquad (4)$$

$$TR_i^j = TR_i^j + \lambda \quad (0<\lambda<1) \qquad (5)$$

### 4.3 Decision module

The decision module is responsible for making an appropriate decision after it receives an updated TR. If the updated $TR_i^j$ is less than the lowest threshold $T_{evil}$ (0.3), vehicle i adds j into its local blacklist and refuses to exchange messages with j. Otherwise, vehicle i defines vehicle j to be normal and transfers messages to j. Besides, vehicle i will update the information of vehicle j in its meeting list.

RSUs gather the local blacklists from vehicles, crosscheck them to verify malicious vehicles and broadcast a warning report. A vehicle which receives warning reports will add attackers into its blacklist. The detailed work of RSU will be done in the future.

## 5 Simulation evaluation

We use The ONE[3]simulator to evaluate the effectiveness of our MDS. In the simulations, 40 nodes with a transmission radius of 100 meters and a moving speed varying from 10 km/h to 50 km/h and a buffer size of 10MB are uniformly deployed in the Helsinki city map with a size of 4500m×3400m to simulate VDTNs. We assume nodes follow the shortest path map based movement routing and generate messages in a interval between 25 to 30 seconds. We have not yet implemented the RSU functionality in this simulation. The simulation time is 12 hours (43200s) and vehicles apply MDS starting from second 10000. We randomly choose 4, 8 and 12 nodes among those 40 nodes as blackholes to evaluate our MDS.

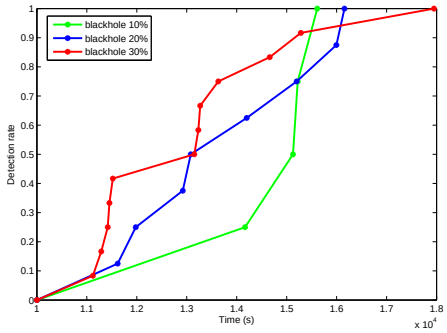


Figure 2: Detection rate

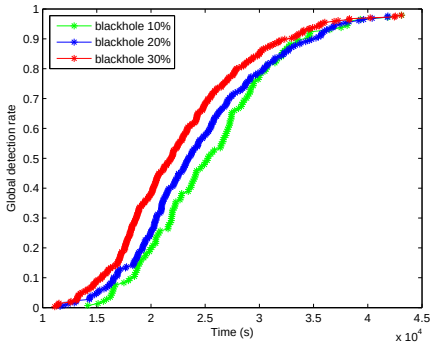


Figure 3: Global detection rate

Table 1
Detection rate, global detection rate and false positive rate

| Percentage of blackhole | Detection rate | Global detection rate | False positive rate |
|---|---|---|---|
| 10% blackhole | 100% | 97.92% | 0 |
| 20% blackhole | 100% | 97.66% | 0 |
| 30% blackhole | 100% | 97.92% | 0 |

We use the following metrics to evaluate our MDS. 1) Detection rate, which is defined as the percentage of evil nodes that are detected by another node in the system. 2) Global detection rate, which is defined as the percentage of evil nodes that are detected by all

[3] http://www.netlab.tkk.fi/tutkimus/dtn/theone/

good nodes. 3) False positive rate, which is the percentage of legitimate nodes that are mistakenly detected as evil nodes.

We study the detection rate versus different number of malicious nodes in the system, as shown in Table 1. When the percentage of blackholes increases from 10% to 30%, comparing detection rate with [RCYC10] and [LC12] our MDS can still consistently achieve a high detection rate without false positive. Figure 2 illustrates that with 4 blackholes, it takes around 5612 s to detect all blackholes. As the density of blackholes increases, the detection time rises. But with more blacklisted blackholes, there will be less communication opportunities with blackholes in the system.

As shown in Figure 3, because of the large simulation area and limited simulation time, some of the normal nodes cannot meet all the malicious nodes or need much more time to detect all blackholes. In our experiment the global detection rate is around 97.6%. The presented detection rate, global detection rate and false positive rate indicate that our MDS design is suitable to detect blackholes.

## 6 Conclusion and future work

By using our MDS, vehicles can independently detect malicious and selfish vehicles, isolate them and prevent them from disrupting the network. Our MDS achieves a high detection rate and a low false positive rate when detecting blackholes. In future work, we will consider other types of misbehaviors and enhance the detection speed of our system.

## References


[D09] Davies,E.: DTN - The State of the Art, http://www.n4c.eu/, 2009.

[AKGOL07] Asokan,N.;Kostiainen,K.;Ginzboorg,P.;Ott,J.; Luo,C.: Applicability of identity-based cryptography for disruption-tolerant networking, Proceedings of the 1st international MobiSys workshop on Mobile opportunistic networking, NY, USA, Jun. 2007; pp. 52-56.

[MGLB00] Marti, S.; Giuli, T. J.; Lai, K. and Baker, M.: Mitigating Routing Misbehavior in Mobile Ad Hoc Networks, Proceedings of the 6th Annual International Conference on Mobile Computing and Networking, Boston, USA, Aug. 2000; pp. 255-265.

[BB02] Buchegger,S. and Boudec, J.Le: Performance Analysis of the CONFIDANT Protocol, Proceedings of the 3rd ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc'02), Lausanne, Switzerland, Jun. 2002; pp. 226-336.

[RPAJH07] Raya, M.; Papadimitratos, P.; Aad, I.; Jungels, D.; Hubaux, J.-P.: Eviction of Misbehaving and Faulty Nodes in Vehicular Networks, IEEE Journal on Selected Areas in Communications, Special Issue on Vehicular Networks, Oct. 2007; 25(8):1557–1568.

[RCYC10] Ren, Y.; Chuah, M. C.; Yang, J.; Chen, Y.: Detecting blackhole attacks in disruption-tolerant networks through packet exchange recording, in Proc. of 1st Workshop D-SPAN (colocated with WoWMoM), Montreal, QC, Canada, Jun. 2010; pp. 1-6.

[LC12] Li,Q. and Cao, G.:Mitigating Routing Misbehavior in Disruption Tolerant Networks. IEEE Transaction on Information Forensics and Security, 2012; 7(2): 664-675.

[CY06] Chuah, M. and Yang, P.: Comparison of Two Intrusion Detection Schemes for Sparsely Connected Ad Hoc Networks, Proceedings of IEEE Milcom, Washington DC, Oct. 2006; pp. 1-7.