Durham Research Online

Deposited in DRO:
05 June 2018

Version of attached file:
Accepted Version

Peer-review status of attached file:
Peer-reviewed

Citation for published item:

Further information on publisher’s website:
https://doi.org/10.1109/infcomw.2018.8406818

Publisher’s copyright statement:
© 2018 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works.

Additional information:

Use policy

The full-text may be used and/or reproduced, and given to third parties in any format or medium, without prior permission or charge, for personal research or study, educational, or not-for-profit purposes provided that:

- a full bibliographic reference is made to the original source
- a link is made to the metadata record in DRO
- the full-text is not changed in any way

The full-text must not be sold in any format or medium without the formal permission of the copyright holders.

Please consult the full DRO policy for further details.
Performance Analysis of Behavior-based Solutions in Vehicular Networks

Aljawarah Alnasser, and Hongjian Sun

Abstract—Transportation systems require communication network for achieving safe traffic and efficient transportation. As a result, vehicles become exposed to either internal or external attacks. Various behavior-based methods were proposed to protect vehicular networks against internal attacks. In this paper, we propose two behavior-based models that apply different methods which are weighted-sum and fuzzy logic. We conduct various experiments using different communication and behavioral scenarios. In addition, we analyse the results to measure the performance of both methods. Simulation results show that weighted-sum method outperforms fuzzy logic in vehicular networks. A comparison result present that the detection rate improves for weighted-sum method with almost all scenarios. Indeed, the detection rate for scenario 1, when there is no direct communication with malicious node, is improved by at least 27%.

Index Terms—VANETs, Weighted-sum, Fuzzy logic, Trust.

I. INTRODUCTION

During recent years, vehicles’ manufacturers have started working on developing the traditional transportation system and transforming it into an intelligent system. This is achieved by embedding extra hardware such as sensors and communication interface within each vehicle and combining them with a software system. Thus, the vehicles can sense the surrounding environment and share the collected information with neighboring vehicles using wireless communications. Also, they can process the information and make a decision without any external intervention.

Vehicular Adhoc NETwork (VANET) is the initial design of vehicular networks. It provided the chance to develop much research and suggest various applications for vehicular networks. It supports ad-hoc communication between vehicles and Road Side Units (RSUs). In VANETs, the vehicles can share information with their neighboring vehicles using two types of communications [1] as shown in Fig.1: Vehicle-to-Vehicle (V2V) supports the communications between vehicles, and Vehicle-to-Infrastructure (V2I) provides communications between vehicles and infrastructure units that are located in the roadside. The communication is established using Dedicated Short Range Communications (DSRC) technology which uses IEEE 802.11p. Vehicles use multi-hop routing protocol to transmit the packet through the network.

As a result, similar to the existing wireless networks, VANETs are vulnerable to various cyber-attacks because the physical access is not required to gain access to the network. Cyber-attacks can be divided into external attacks and internal attacks. The external attacks are launched by nodes that do not belong to the network. While, the internal attacks are executed by compromised or hijacked nodes that belong to the network.

Internal attacks are typically hard to detect since malicious nodes already belong to the network as authorized nodes. Thus, these nodes require being protected by implementing a security system. Therefore, traditional security mechanisms are not suitable for addressing these attacks [2]. Various behavior-based solutions were proposed for addressing the internal attacks. Each node observes the behavior of its neighboring nodes and reports any malicious activity.

There are various methods that were suggested as behavior-based solutions as follows:

- The weighted-sum method is the common behavior-based method. Trust evaluation is computed by assigning different weights for each trust component. Total trust is computed by:

$$T_{total} = \sum_{i=1}^{U} w_i \times T_x$$

where $w_i$ is a weight value for $T_x$, $T_x$ is a trust value for trust level $x$ such as direct trust and indirect trust, and $U$ is the number of trust levels that will be considered. For instance, Patel and Jhaveri [3] applied the weighted-sum method with Ant Colony Optimization (ACO) algorithm for forwarding packets through the shortest trusted path by isolating non-cooperative nodes. The main drawback
is that even if all node’s neighbors are malicious, it is enforced to forward the packets to one of them. Moreover, Wei et al. [4] proposed a trust model for detecting non-cooperative nodes on V2V communications only. Also, it was used for checking data integrity in [5] [6].

- The fuzzy logic method incorporates a series of IF-THEN rules to solve a control problem rather than attempt to model a system mathematically. The main steps of the fuzzy logic model are as follows [7]. First, the fuzzy sets and criteria are defined; next, the input variable values are initialized; then, the fuzzy engine applies the fuzzy rules to determine the output data and evaluate the results. Fuzzy logic models were proposed in [8] and [9] to detect dropping and modification message respectively. Moreover, Ding et al. [10] proposed a fuzzy reputation based model to prevent the spreading of false messages.

A. Contributions and Structure

The main goal of this paper is studying the performance of various behavior-based methods in vehicular networks which are the weighted-sum and fuzzy logic. This paper makes three significant contributions to the field of vehicular network security:

1) The performance of the common behavior-based methods in vehicular networks is studied.
2) The various communication scenarios with malicious node are examined and analyzed.
3) The effect of different patterns of malicious behavior is studied.

The paper is organized as follows: in section II we provide a detailed description of the proposed behavior based model. In section III we present the simulation setup parameters and discuss the simulation results. In section IV we measure the model performance for both proposed methods.

II. PROPOSED SYSTEM MODEL

A. Considered Network

The considered network consists of N vehicles and M RSUs along the road. The vehicles move with a random speed where they are restricted by road directions. The vehicles keep recording data which is pertinent to traffic events and share them with neighboring vehicles and RSUs through the formed mesh network. The network considers two types of nodes as follows.

1) Normal node: keeps monitoring the surrounding environment and broadcasts warning packets when an event is triggered. The events are randomly distributed as shown in Algorithm 1. The warning packet is generated and sent to the other vehicles through the use of a multi-hop routing protocol. Moreover, the event’s location is randomly distributed.

2) Malicious nodes: multihop networks, such as vehicular networks, depend on that the neighboring nodes will truly forward their messages through the network. However, unfortunately, this is not the case in greyhole attack. In greyhole attacks, malicious nodes stop forwarding some packets, and this makes detection of these malicious nodes difficult. This attack can isolate some nodes, and that affect the data accuracy.

B. Model Structure

Our behavior-based model measures trustworthiness level for all vehicles in the network. The trustworthiness is evaluated based on the information that is obtained through direct observation of one-hop neighbors. Indeed, the vehicle with low trust value is considered untrusted node. The proposed model manages two trust components as follows.

1) Direct trust ($D_{i,j}^{(t)}$): as mentioned before, VANET is a multi-hop network where vehicles are responsible for forwarding the packets to the neighboring vehicles. Each vehicle is able to compute the direct trust of its one-hop neighbors through direct observations for the considered node, then, it sends these values to the nearest RSU. For example, node $i$ forwards the packets to its neighbor node $j$ and keeps monitoring node $j$ to verify whether it forwards the packets. The direct trust $D_{i,j}^{(t)}$ between node $i$ and node $j$ at time $(t)$ is measured by

$$D_{i,j}^{(t)} = \frac{\text{forwarded}_i}{\text{Total}_i}$$

where $\text{forwarded}_i$ is the number of packets that node $j$ received from node $i$ and forwarded them successfully. $\text{Total}_i$ is the total packets that node $j$ received from node $i$.

2) Indirect trust ($I_{RSU,j}^{(t)}$): each RSU broadcasts a request periodically to collect direct trust values from all nodes in its transmission range. RSUs are responsible for computing indirect trust and broadcasting it to all nodes in the network [15]. RSUs are interconnected with each others through a wired connection. Thus, each RSU can fill the matrix with the nodes’ feedback using

$$Feedback = \begin{bmatrix}
D_{1,1}^{(t)} & \cdots & D_{1,n}^{(t)} \\
\vdots & \ddots & \vdots \\
D_{n,1}^{(t)} & \cdots & D_{n,n}^{(t)}
\end{bmatrix}$$

where $n$ is the number of vehicles in the network. Indirect trust $I_{RSU,j}^{(t)}$ between RSU and node $j$ at time $(t)$ is computed by

$$I_{RSU,j}^{(t)} = \frac{\sum_{k=1}^{m}(D_{k,j}^{(t)})}{m}$$

where $m$ is the number of nodes that have a feedback about node $j$, $m \leq n$.

Input: $\lambda, \Delta$

Output: $V$

1: for each time interval do
2: $p = rand[0, 1]$;
3: if ($p < \lambda \times \Delta$) then
4: $V=Event();$
5: $V.Location_{X} = rand[0, 900];$
6: $V.Location_{Y} = rand[0, 900];$
7: $V.existing = True;$
8: end if
9: end for
10: return $V$

Algorithm 1: Algorithm for event distribution variables
C. Proposed Behavior-based Methods

1) The weighted-sum method: trust evaluation is computed by assigning different weights to each trust level. When the node behaves maliciously; the total trust value decreases until reaches to zero [16]. Total trust \((Total_{i,j}^{(t)})\) for node \(i\) about node \(j\) at time \((t)\) is computed by:

\[
Total_{i,j}^{(t)} = w_1 \times D_{i,j}^{(t)} + w_2 \times I_{RSU,j}^{(t)}
\]

where \(w_1\) and \(w_2\) are weights for direct and indirect trust respectively, and they are equal to 0.5. At time \((t)\), if node \(i\) does not communicate with node \(j\), node \(i\) evaluates node \(j\) based on the indirect trust only.

2) The fuzzy logic method: is composed of the following four steps.

1) Linguistic inputs (trust components): as shown in Fig. 2, the model has two inputs which represent trust components: direct trust and indirect trust. At time \((t)\), if node \(i\) does not communicate with node \(j\), node \(i\) uses the previous direct trust value \(D_{i,j}^{(t-1)}\) to evaluate node \(j\).

2) Fuzzification Process: the input linguistic variables are connected through AND logical operator. The proposed model uses membership functions which were proposed in [17].

3) Fuzzy Interference Rule-Base: trust values are calculated by passing the fuzzy sets described in [17] through fuzzy inference rules. Total trust \((T_{total}^{(t)})\) uses Triangular and Trapezoidal Membership Functions which are specified by three parameters [17]: Malicious, Less Trusted, Normal. The number of the input linguistic variables is two in the proposed method and each variable takes three values. Thus, the total number of rules, with all possible combinations, is 9.

4) Defuzzification (Total Trust - \(T_{total}^{(t)})\): after fuzzification, the next step is a defuzzification to get crisp values using mathematical method.

III. Simulation Analysis

This section describes the experimental setup used to measure and study the efficiency of two behavior-based methods: weighted-sum and fuzzy logic. Various communication and behavioral scenarios are evaluated in this section.

A. Network specifications

In our simulation model, we consider a VANET with fifteen vehicles which included one malicious node with parameters as shown in Table I. The vehicles move over an area of \(900 \times 900 m^2\) with three random speed ranges. The considered area is composed of two intersections using three one-lane roads, where one RSU is located at each intersection. The system operates on an event basis, such that each vehicle continuously monitors a surrounding area and sends a warning message only when the traffic event occurs.

To measure the performance of various behavior-based methods, we assume that the malicious node launches a greyhole attack. Also, when no event is triggered at time \((t)\), RSUs use the recorded trust value at time \((t-1)\).

B. Results for various communication scenarios

To study the method performance, we examine different communication scenarios with malicious node as follows.

1) Scenario B1: there is no direct communication between normal node \(i\) and malicious node \(j\): in this scenario, we examine the ability of normal node \(i\) to detect malicious node \(j\) while it does not have any past experience with it. In weighted-sum model, normal node \(i\) is not able to compute direct trust for malicious node \(j\) in this scenario. Therefore, total trust is equal to indirect trust. On the other hand, in the fuzzy logic method, the normal node \(i\) uses the direct trust value of malicious node \(j\) that was computed in the previous interval. The corresponding result is shown in Fig.3. The following remarks can be made:

- in weighted-sum model, trust value drops to zero because the total trust totally depends on indirect trust. While in fuzzy logic, we notice that trust value decreases to 0.5;
- after the 15th interval, trust value in both models increases, however, fuzzy logic gives higher values;
- the detection of malicious node in fuzzy logic model is more difficult compared with weighted-sum method.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Simulation time (T)</td>
<td>10 sec</td>
</tr>
<tr>
<td>No. of simulation steps (N)</td>
<td>100 steps</td>
</tr>
<tr>
<td>Simulation step size (Δt)</td>
<td>0.1 sec</td>
</tr>
<tr>
<td>Arrival rate (λ)</td>
<td>0.1 sec</td>
</tr>
<tr>
<td>Speed ranges</td>
<td>(10-50), (20-60), (10-30)</td>
</tr>
<tr>
<td>Number of nodes</td>
<td>15 (one malicious node)</td>
</tr>
<tr>
<td>Total(_{i,j}^{(0)})</td>
<td>0.8</td>
</tr>
</tbody>
</table>
2) Scenario B2: the normal node i communicates with malicious node j at the beginning of simulation time: in this scenario, we examine the effect of the communication with malicious node at the beginning of simulation time on the detection rate. The normal node i communicates with malicious node j at the 10th interval. From the results in Fig.4, we can conclude the following:

- before the 10th interval, there is no direct communication with malicious node. Thus, it is assumed to be affected by indirect trust value in both models;
- after the 10th interval, the total trust for both models depends on direct and indirect trust values;
- we notice that the trust values in both models are very close to each others.

3) Scenario B3: the normal node i communicates with malicious node j at the end of simulation time: in this scenario, we examine the effect of late connection between normal node i and malicious node j. The normal node i communicates with malicious node j at the 71st interval. From the results in Fig.5, we can conclude the following:

- before the 71st interval, there is no direct communication with malicious node. Thus, it is assumed to be affected by indirect trust value in both models;
- after the 71st interval, the total trust for both models drops to approximately 0.3. In addition, we notice that the trust values for both models are very close to each others.

C. Results for different patterns of malicious behavior

We examine various patterns of malicious behavior and analyse them to measure how could they affect on the detection rate. The malicious behavior scenarios are as follows.

1) Scenario C1: non-stable malicious behavior: in this scenario, at the 20th interval, malicious node j behaves normally with neighboring nodes for five intervals. Then, it starts malicious behavior after the 25th interval. The corresponding result is shown in Fig.6. The following remarks can be made:

- after the 20th interval, trust value increases for both models until reach 0.86;
- when malicious node j behaves maliciously at the 26th interval, the trust value decreases for both models;
- we notice that trust values for both models follow the same pattern.

2) Scenario C2: malicious node behaves normally: in this scenario, there is no direct communication with malicious node j until the 71st interval. After that interval, the malicious node starts to behave normally with other nodes. From the result in Fig.7, we can conclude the following:

- before the 71st interval, the trust value is affected by indirect trust in both models;
- after the 71st interval, we notice that trust value increases because of the normal behavior;
- we notice that fuzzy logic give higher trust value than weighted-sum in this scenario.
IV. PERFORMANCE ANALYSIS

In this section, we analyse the results to measure the performance of the two proposed methods. In addition, the false negative rate for both methods is examined.

A. Performance analysis for false negative rate

We measure the false negative rate in weighted-sum method and fuzzy logic. The False Negative Rate (FNR) measures the percentage of undetected attacks. It is computed by

\[
FNR = \left( \frac{FN}{Total\,attacks} \right) \times 100
\]

where FN is a false negative.

Behavioral-based model applies predefined trust threshold to be able to make a decision about malicious behavior. If trust value of node \( j \) is below a specific threshold, node \( j \) is marked as a malicious node. To get the following results, we assumed that trust threshold is equal to 0.6.

1) Study for various communication scenarios: from the result in Fig.8, we can conclude the following:

- in the first scenario, when no communication with malicious node, we notice that the false negative rate is very high in fuzzy logic compared with weighted-sum;
- when the malicious behavior is launched at the beginning of time, both models have the ability to detect the malicious node. On the other hand, the false negative rate approximately is equal to an average value for both models when the malicious behavior starts at late intervals.

2) Study for various malicious behavior patterns: from the result in Fig.9, we can conclude the following:

- the false negative rate in the first scenario, when non-stable malicious behavior is applied, is less than in the second scenario with normal behavior of malicious node;
- it is expected to have high false negative rate in the second scenario because no malicious behavior is initiated.

B. Improvement measurement

From the previous section, we notice that weighted-sum method gives us more accurate detection than the fuzzy logic. Consequently, we measure the improvement percentage of detection rate in case of greyhole attack for weighted-sum method compared with fuzzy logic. From the result in Fig.10, we can conclude the following:

- The best performance of weighted-sum in the first scenario when there is no communication with malicious node.
- The worst performance of weighted-sum when malicious node initiates non-stable malicious behavior, where the improvement for the most of the time is less than or equal to 10%.
- After a long time, the improvement percentage for all scenarios are close to each other except no direct communication scenario where the detection rate improves with time.

V. CONCLUSION

In this paper, we proposed two behavior-based models which are weighted-sum and fuzzy logic. We conducted various experiments to study the performance of both models. Also, we considered different communication scenarios with malicious node that launches greyhole attack. Simulation results showed that weighted-sum method outperforms fuzzy logic in VANETs. A comparison result showed that the detection rate improves for weighted-sum method with almost all scenarios. The detection rate for scenario 1, when there is no direct communication, was improved by at least 27%.
At the end No communication At the beginning Non-stable behavior Normal behavior

Fig. 10. Improvement percentage of weighted-sum method compared with the fuzzy logic.

In future work, we will apply the proposed model in Vehicle-to-Everything (V2X) network and compare the results. The proposed model can be combined with cloud computing as a central storage for trust values.

REFERENCES


