2018 IEEE Intelligent Vehicles Symposium (IV)
Changshu, Suzhou, China, June 26-30, 2018

A Security Aware Fuzzy Enhanced Reliable Ant Colony Optimization Routing in Vehicular Ad hoc Networks

Hang Zhang, Arne Bochem, Xu Sun and Dieter Hogrefe
Institute of Computer Science, Telematics Group
University of Goettingen, Germany
{hang.zhang,bochem,hogrefe}@cs.uni-goettingen.de
xu.sun@stud.uni-goettingen.de

***Abstract*—With the growing relevance for Vehicular Ad Hoc Networks (VANETs), the number of applications for such networks also grows. These networks allow vehicles to coordinate, improving both efficiency and safety of road traffic. To make such networks feasible, efficient routing protocols that are robust against malfunctioning or malicious network participants are required. Additionally, the routing algorithm has to be able to cope with the transient nature of connections in VANETs as vehicles pass by each other at high speeds. In this work, we propose the Security Aware Fuzzy Enhanced Reliable Ant Colony Optimization (SAFERACO) routing protocol which makes use of a fuzzy logic module to identify misbehaving nodes and exclude them from the routing process. We implement SAFERACO in the NS-3 simulator and evaluate it under different scenarios. The results show superior performance in all relevant metrics, such as packet delivery rate and delay. Due to its ability to identify misbehaving nodes, SAFERACO also provides a high level of robustness against black hole and flooding attacks.**

***Index Terms*—ACO, Routing, VANETs, Fuzzy logic, Security, MANETs**

I. Introduction

Vehicular Ad Hoc Networks (VANETs) [18] consist of collections of mobile vehicles and are becoming a new emerging branch of wireless technology which derives from Mobile Ad-hoc NETworks (MANETs) [12]. Although VANETs have several similarities to MANETs, they are distinguished from other kinds of MANETs by their vehicle movement properties (e.g. high speed), hybrid network architectures and practical application scenarios. There are various application in VANETs, the main one being Intelligent Transportation Systems (ITS) [11]. ITS is not a single application, but rather includes a variety of applications, such as co-operative traffic monitoring, the control of traffic flows, prevention of collisions, nearby information services, providing Internet connectivity to vehicles and so on. Due to the high mobility and unreliable channel conditions, VANETs have many unique characteristics, which pose many challenging research issues when implementing functionality, such as data dissemination and data sharing. Security is another important issue, as unreliability might lead to dangerous situations in road traffic. As the applications in VANETs become increasingly more widespread, attackers are also more motivated to manipulate or disrupt the communications in VANET applications. Therefore, the design of efficient and secure routing protocols for VANETs is very important.

The Ant Colony Optimization (ACO) meta-heuristic [4] has shown the ability to efficiently find optimal routes in MANETs, while also being able to adapt to the constantly changing topology of dynamic networks. It is inspired by biology and follows the approach that ants use in finding efficient paths, by tracking pheromones deposited along the way, which applies as well in networks as it does in nature. Inspired by the ACO meta-heuristic, in this paper we propose a Security Aware Fuzzy Enhanced Reliable Ant Colony Optimization (SAFERACO) routing protocol for VANETs. SAFERACO aims to provide efficient and secure routing in VANETs. It employs a distributed fuzzy logic module to evaluate the behavior of nodes in the network, assigns reliability scores to neighboring nodes and is able to exclude misbehaving nodes from the routing process. We evaluate our approach and show its effectiveness in routing and its ability to robustly perform under black hole [2] and flooding attacks [17], showing its high level of security.

This paper is organized as follows: Section II reviews related work. Our proposed SAFERACO routing algorithm is described in detail in Section III. Section IV provides a detailed evaluation of our approach, showing its performance characteristics. Finally, we give our conclusions and point out future directions of research in Section V.

II. Related Works

Routing is a core issue for allowing a network to communicate. However, due to the dynamic nature of the VANETs, discovery and maintenance of routes is a very challenging task. To solve this issue, a variety of different routing

978-1-5386-4451-5/18/$31.00 ©2018 IEEE

protocols have been proposed. They generally fit into five categories: ad hoc, position-based, cluster-based, broadcast, and geocast routing [11].

Ad hoc routing protocols for VANETs are mainly the ones which are originally designed for MANETs, such as the Ad-hoc On-demand Distance Vector (AODV) protocol [14] and Dynamic Source Routing (DSR) [7]. VANETs have many similarities to other types of MANETS, such as not relying on fixed infrastructure, having low bandwidth, short radio transmission range and so on. However, vehicles in VANETs move much faster than the normal mobile nodes in MANETs, which can lead to poor performance of MANET algorithms in VANETs.

In position based routing protocols, nodes use location information to help facilitate communications. For examples, in greedy routing nodes always forward the packets to the node that has the shortest geographical distance to the destination. Greedy Perimeter Stateless Routing (GPSR) [8] is one of the representative position-based protocols in literature. In GPSR there is no need to establish a global route from source nodes to directly to destination nodes, which can reduce the processing costs of system. In city scenarios however, GPSR can suffer from several problems, due to the presence of obstacles and mobility leading to routing loops [11].

Cluster-based routing attempts to provide scalability by creating a virtual hierarchical network infrastructure through the clustering of nodes. Vehicles are divided into clusters with cluster heads that coordinate intra- and inter-cluster communications. While vehicles inside a cluster communicate with each other directly, the communications between clusters are performed via the cluster-heads or the cluster gateways. Santos et al. [15] have proposed a reactive location based routing algorithm for VANETs called CBLR. It assumes that all nodes can gather their position information by GPS to build the clusters. Simulation results show that CBLR can achieve good scalability for large networks. However, forming and maintaining clusters causes extra overhead. Moreover, cluster-based routing protocols also rely on the geographical information of vehicles to create stable clusters, which may not always be reliable or available.

Broadcast based routing protocols, such as the Urban Multi-Hop Broadcast protocol (UMB) [9], transmits data to all available nodes within communication range over the entire network. This kind of routing performs relatively well for VANETs with a limited small number of vehicles and is easy to implement. However, when the number of vehicles in the network increases, the bandwidth requirements increase exponentially. Moreover, since each node receives and re-broadcasts every message almost at the same time, it leads to packet collisions and network congestion, which may cause a high amount of additional overhead.

Geocast routing [13] is basically a location-based multicast routing approach that aims to deliver packets from a source vehicle to all other vehicles within a predefined geographical zone. While useful for use cases such as emergency broadcasts, the communication range is limited by the Zone Of Relevance (ZOR) and it is mainly designed for unidirectional message dissemination in one single region, not for pairwise communication in the network.

As mentioned, MANET routing approaches can also be applicable to VANETs. Caro et. al. propose a MANETs routing protocol called AntHocNet [3], which is based on the Ant Colony Optimization (ACO) meta-heuristic. The ACO meta-heuristic presents a common framework for approximating solutions to NP-hard optimization problems. AntHocNet is a hybrid routing approach, in which reactive ants are used to discover new routes, while proactive ants are used to explore alternative routes during data transmissions. A comprehensive overview of ACO based routing approaches is presented by Zhang et al.[20] in 2017.

III. SAFERACO Routing in MANETs

Inspired by other ACO routing algorithms, we propose the Security Aware Fuzzy Enhanced Reliable Ant Colony Optimization (SAFERACO) routing protocol for use in VANETs. SAFERACO is based on the Security Aware Fuzzy Enhanced Ant Colony Optimization (SAFEACO) routing protocol first proposed by Zhang et al. [19], but includes additional protection against flooding attacks and has been evaluated especially for the use in VANETs. Our aim is to design a routing protocol in Vehicle to Vehicle (V2V) networks which can provide a high packet delivery ratio, low end-to-end delay and low communication overhead in both normal and attack scenarios.

Since AntHocNet, with its hybrid architecture, shows convincing performance and it has been proven to be efficient in MANETs, we apply its routing structure in SAFERACO. The core processes in SAFERACO routing protocol are the reactive route setup and the proactive route maintenance.

A. Reactive Route Setup in SAFERACO

In order to find a route, the source vehicle broadcasts reactive Forward ANTs (FANTs). Ants choose the next hop by following the probabilistic decision rule which is described in Equation 1.

$$P_{ij}^{d}(t) = \frac{\left[\tau_{ij}^{d}(t) \cdot R_{ij}(t)\right]^{\alpha}}{\sum_{l \in N_i^d} \left[\tau_{il(t)}^{d} \cdot R_{il}(t)\right]^{\alpha}} \quad \text{if} \quad j \in N_i^d \qquad (1)$$

where $P_{ij}^{d}(t)$ is the probability of an ant moving from vehicle i to vehicle j on the way to the destination vehicle d at the t-th iteration step or time slot; N_i^d is the set of current

neighboring vehicles of vehicle i, over which a route to vehicle d is known; $\tau_{ij}^{d}(t)$ is the regular pheromone intensity on the link between vehicles i and j on the way to destination vehicle d at t-th iteration step or time slot; $R_{ij}(t)$ is the reliability value estimated by the fuzzy detection system in Section III-C for the link between vehicles i and j at the t-th iteration step or time slot; $\alpha \geqslant 1$, is a parameter which can control the exploratory behavior of the ants. α is set to 20 in our experiments, which is the same value used in AntHocNet [5].

At each intermediate vehicle, the reactive FANT is either unicast or broadcast, depending on whether the current vehicle has routing information for the destination. In order to limit the overhead caused by broadcasting ants, intermediate vehicles only forward the first copy of any received ants. A reactive FANT moves hop by hop until it reaches the destination vehicle or the maximum travel hop count of the ant is reached. For each step, it chooses one of its neighbor vehicles according to Equation 1.

After the ant arrives at the destination vehicle, it turns into a backward ant (BANT) and travels back to the source vehicle by following exactly the same route. At each intermediate vehicle, the BANT updates the cost value C_{id} by adding the last hop's cost value C_{in} to it. C_{id} represents the cost of sending a packet from vehicle i to vehicle d along this route. The amount of pheromone updates assigned to a link is calculated based on the quality of the route in which this link is involved, and the pheromone evaporation rate, as shown in Equation 2. An ant considers the quality of a route to be inversely proportional to the cost of the route C_{id}. The pheromone evaporation rate is predefined and allows ants to forget outdated routes and to explore new routes.

$$\tau_{ij}^{\text{new}} = \rho \cdot \tau_{ij}^{\text{old}} + (1-\rho) \cdot \frac{1}{C_{id}} \tag{2}$$

τ_{ij}^{old} is the previous regular pheromone value on the link between vehicles i and j; τ_{ij}^{new} is the updated regular pheromone value on the link between vehicles i and j; $\rho \in (0, 1]$ is the pheromone evaporation rate. In our experiments, ρ is set to 0.7, which is as the same as in AntHocNet [5]. C_{id} is calculated based on the signal-to-noise ratio (SNR) as shown in Equation 3.

$$C_{ij} = \begin{cases} 1 & \text{if} \quad \text{SNR} > \text{SNR}_t \\ C_{\text{const}} & \text{if} \quad \text{SNR} \leqslant \text{SNR}_t \end{cases} \tag{3}$$

SNR_t is the predefined threshold value for the SNR, at which a link is considered as bad; C_{const} is the cost of using a bad link. In our experiments, we fellow the original AntHocNet implementation [5] and keep SNR_t set to 17 dB and C_{const} set to 3.

After the route to the destination is discovered successfully, data packets are forwarded in the same way as the regular forward ants, i.e. by applying Equation 1. The link failure mechanism implemented in SAFERACO handles updating the pheromone tables of affected vehicles, when link failures occur. It is based on the one in AntHocNet [5]. Therefore, we will not specially introduce it in this paper.

B. Proactive Route Maintenance in SAFERACO

In order to improve routing efficiency, we also propose a proactive route maintenance mechanism in SAFERACO. It consists of two parts: pheromone diffusion and proactive ant sampling. In the first process, vehicle i, chooses randomly up to 10 destinations to which it has valid routing information and distributes the routing information in the hello message to its neighboring vehicles. After receiving the hello message, neighboring vehicle j estimates a virtual (or bootstrapped) pheromone value from itself to each reported destination vehicle in the hello message. The exact formula is given in Equation 4.

$$\omega_{ji}^{d} = ((V_i^d)^{-1} + C_j^i)^{-1} \tag{4}$$

ω_{ji}^{d} denotes the bootstrapped pheromone value of vehicle j to destination d via neighbor vehicle i; V_i^d is the reported pheromone value of this route, which indicates the quality of the best route from vehicle i to vehicle d; C_j^i is the locally maintained cost value of hopping from vehicle j to vehicle i.

The additional overhead caused by this step is negligible, because adding the table to the hello message only increases its size by a few bytes. No additional control packets need to be sent out, so no additional media access control overhead is introduced either.

In the proactive ant sampling process, source vehicles send proactive forward ants regularly to gather routing information for ongoing data sessions. In our experiments, during data sessions, proactive forward ants are sent out every second. Proactive forward ants apply a probability rule described in Equation 5 to choose their next hop.

$$P_{ij}^{d}(t) = \frac{(\max\left[\tau_{ij}^{d}(t), \omega_{ij}^{d}(t)\right] \cdot R_{ij}(t))^{\alpha}}{\sum_{l \in N_i^d} (\max\left[\tau_{il(t)}^{d}, \omega_{il}^{d}(t)\right] \cdot R_{ij}(t))^{\alpha}} \quad \text{if} \quad j \in N_i^d \tag{5}$$

In our experiments, the α used in Equation 5 is set to 2. Once the proactive ant reaches its destination vehicle, it is converted into a proactive backward ant which has the same behavior as reactive backward ants. It updates the regular pheromone values on its way back to its source node. In this way, the proactive ant sampling process can investigate the

attractiveness of virtual pheromone values obtained from the pheromone diffusion process and, if the proactive backward ant comes back, a new route is found for data transmission.

C. Fuzzy Logic Based Detection System

We employ a distributed fuzzy logic based misbehavior detection system to protect the network from malicious actors and attacks. MANETs are, as indicated by their name, mobile, so usually only limited information about the surrounding environment is available. Reasoning with only information about e.g. neighboring nodes can be difficult for traditional approaches and provides insufficient amounts of data to perform online machine learning on nodes. These circumstances make fuzzy logic an appropriate choice, as fuzzy inference systems can operate with fuzzy data as is usually available in this type of scenario. Benign nodes may drop packets due to channel congestion, interference or collisions, so assigning them a binary ”reliable” flag would not be appropriate, while the softer categorization provided by a fuzzy logic system allows representing these nuances well.

As shown in Figure 1, there are three input values of the detection system. When a node sends a packet to be forwarded by another node, the sending node will keep listening on the radio channel to check if the receiving node actually forwards the packet within one second. Only the most recent 30 packets are watched for in this way by sniffing the link. The ratio of packets forwarded by a node to packets sent to a node corresponds to its *forward rate*. In our fuzzy system, this rate can either be ”low”, ”medium” or ”high”. The second input for our fuzzy system is the *recent transmission*, which is defined as the number of packets sent to a given node for forwarding, no matter if it was actually heard to be forwarded or not. Only packets from the last 30 seconds are considered here. The limitation of a maximum of thirty packets in total being considered, as described with regard to the *forward rate*, also applies. In our fuzzy system, this rate can either be ”low”, ”medium” or ”high”. The third input value is the *incoming rate*, which is the number of received packets from one single neighbor node within a predefined interval. This parameter is an indicator that allows us to detect flooding nodes. In our fuzzy system, this rate can either be ”low”, ”medium” or ”high”. Our fuzzy logic module performs fuzzy inference on our three input values and generates an output value called *reliability*. This output value can be either ”very unreliable”, ”unreliable”, ”neutral”, ”reliable” or ”very reliable”. This output value is then employed to make decisions regarding the routing process. The membership functions of these values are given in Figure 2.

The process of the detection of malicious behavior is shown in Figure 1, the input values are first fuzzified and then, based on a number of predefined rules and the membership function, inferencing is performed. The result of this is then defuzzified, which results in the final *reliability* value used in SAFERACO. The rule base used for inference is described in Table I. In this table, a vector (a, b, c) means, that the *forward rate* is has value a, the *recent transmission* has value b and the *incoming rate* has value c, which possible values being **L**ow, **M**edium and **H**igh.

D. Detection in SAFERACO Routing

In order to isolate the malicious nodes in the routing process, SAFERACO applies a distributed fuzzy logic based malicious behavior detection system based on its traffic monitoring system. In SAFERACO, every node monitors each of its neighbor nodes and passes the observed parameters, namely the forward rate, the number of recent transmissions of packets to be forwarded and the number of received packets from one single neighbor node within a predefined interval, into its fuzzy inference system. The fuzzy inference system estimates the reliability value of the observed neighbor node according to the fuzzy rules. This value represents the quality of the link to this neighbor node and it is used in the route decision process for both reactive and proactive forward ants, as shown in Equation 1 and 5. In our experiments, we set the threshold value of the reliability value to 0.12. All nodes with reliability value which is below the threshold value are considered unreliable and will not be chosen in the route.

Since the traffic monitoring system only observes traffic in the network, the detection system applied in SAFERACO does not lead to any additional control packets in the routing

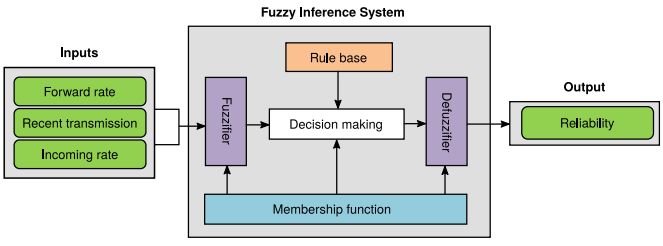

Fig. 1: Block diagram of SAFERACO's fuzzy module.

Reliability	Input combinations
Very reliable	(H, M, L), (H, H, L), (H, M, M), (H, H, M)
Reliable	(M, L, L), (H, L, L), (M, L, M), (H, L, M)
Neutral	(L, L, L), (M, M, L), (L, L, M), (M, M, M)
Unreliable	(M, H, L), (M, H, M)
Very unreliable	In all other cases

TABLE I: Applied fuzzy rules.

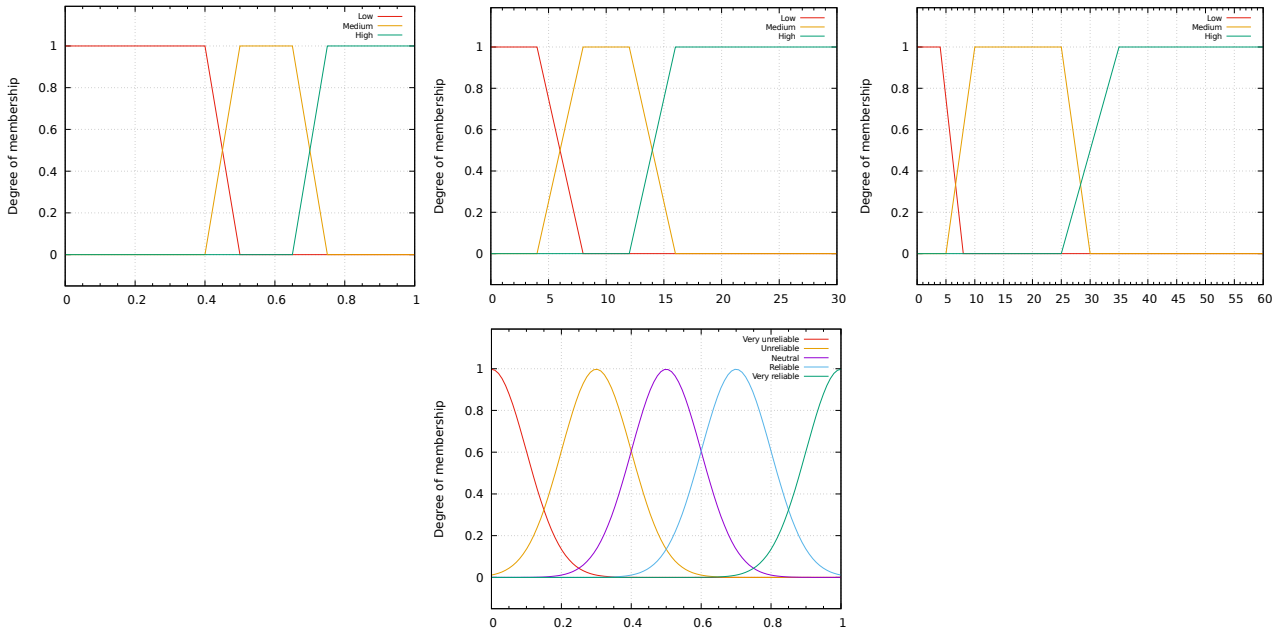

Fig. 2: Membership functions

protocol. However, if a node only has pheromone values for unreliable nodes, it will start a new route discovery process, which may result in additional overhead. The detection system can be adapted to different scenarios. In this work, we chose three input values to detect black hole and flooding attacks. If other attacks against routing protocols should be considered, we can add additional inputs or swap them for existing inputs to our fuzzy detection system. According to the new input values, we then design new fuzzy rules for the fuzzy inference system. This shows the general flexibility of our fuzzy detection system, which allows it to be adapted to handle any concrete demands of an application.

E. Attack Model

1) Black hole attack: Since packet-dropping attacks are a major threat to the operation of MANETs [16], in this work we focus on protecting the network from this kind of attack, exemplified by the black hole attack introduced in [2].

Suppose source node S attempts to find a route to destination node D. S sends out FANTs to discover the network. As soon as black hole node M receives the FANT, it replies immediately with a backwards ant (BANT) which contains a fake route. This fake route will designate itself as the shortest or optimal route. If the source node does not have any mechanism to detect malicious behavior, it will be deceived and will send all data packets to the black hole node, which simply drops them.

2) Ad hoc flooding attack: The main target of the ad hoc flooding attack [17] is to consume network resources, such as bandwidth, to exhaust the energy available to nodes energy or their computational power, to disrupt the routing process in the network. This kind of attack doesn't aim at the resources of some particular nodes, but the resources of the whole network. In this attack mode, a flooding node broadcasts excessive RREQ packets with non-existing destination IP addresses. In this case, no one in the network could reply the these RREQs and as consequence the network will be full of such fake RREQs. In order to make the flooding nodes more difficult to be detected, we let the attack node flood the RREQs in every three seconds in our implementation.

IV. Evaluation

In order to investigate the performance of SAFERACO when undergoing black hole and flooding attacks, we have implement the proposed approach in the NS-3 simulator [1] and compare its performance to that of AntHocNet.

A. Evaluation Measures

Three different measures are chosen for the evaluation of our proposed approach:

1) Packet Delivery Ratio (PDR): This parameter is the total number of packets received by the destination nodes divided by the total number of packets sent by the source nodes. The PDR's value is in the range of $[0, 1]$. Since the

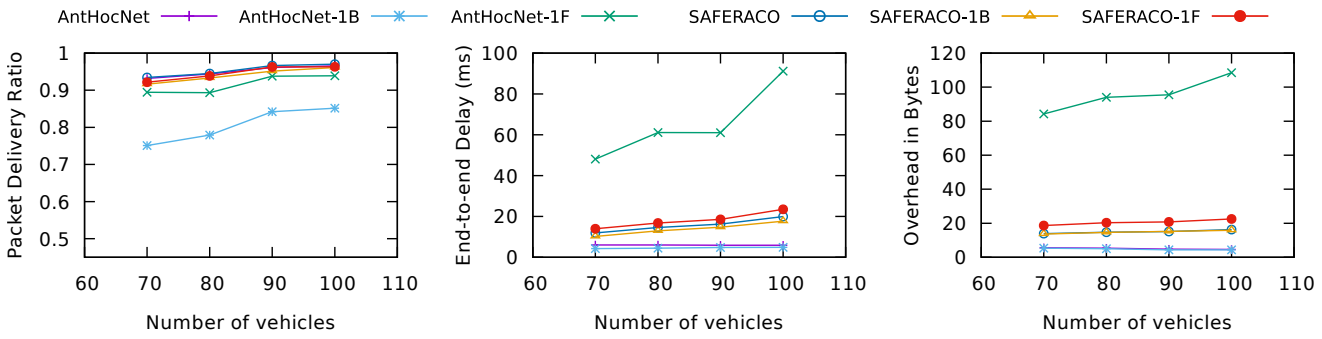

Fig. 3: Comparisons in single attack scenarios.

purpose of a black hole attack is to disturb the communication in the network by dropping packets, ensuring a high PDR value is the main goal of our approach.

2) End-to-end Delay: The delay of a packet is the duration between its sending time and its receiving time. For each simulation run, this value is then averaged over all packets that were actually received in this run. Packets that get dropped during the simulation period are not considered in this measure, because a dropped packet's delay would be infinite and make the measure useless.

3) Overhead: The average overhead is the total number of bytes transmitted in control messages divided by the total number of bytes in delivered data packets. It should be noted that sending a forward ant from the source node to the destination node over n intermediate nodes, is counted as $n + 1$ transmissions, but sending a data packet instead, is counted as one packet being delivery. The overheads caused by the MAC, IPv4 and UDP headers are all included in the calculation.

These three measures are used to quantify the effectiveness of our approach in solving the general routing problem it has been designed to address. Having a high PDR and a low delay measure with low or reasonable overhead would show that SAFERACO is suitable as a routing algorithm in general.

B. Basic Scenario

We employ the Simulation of Urban Mobility (SUMO) [10] traffic simulator in order to simulate a vehicular network scenario. In the basic scenario, there are 70 vehicles in a square area with dimensions of $750\,\mathrm{m} \times 750\,\mathrm{m}$. The map is shown in Figure 4. Each street is bi-directorial and each direction has two lanes. There are 16 traffic conjunctions altogether and the distance between adjacent traffic conjunctions is 250 m. The speed limit in each street is $20\,\mathrm{m/s}$. The traffic lights are setup with default values in SUMO. Radio transmission is modeled according to the Friis propagation model [6], with a transmission power of approximately $20\,\mathrm{dBm}$. There are 10 constant bit rate (CBR) sessions in the network. Each CBR session starts randomly between $0\,\mathrm{s}$ and $30\,\mathrm{s}$. Each source node of a CBR session sends out 4 data packets per second, with a size of $64\,\mathrm{B}$ each. The total duration of each simulation run is set to $1000\,\mathrm{s}$. To collect the data, we performe 10 runs for each scenario with different random seeds and averaged the results.

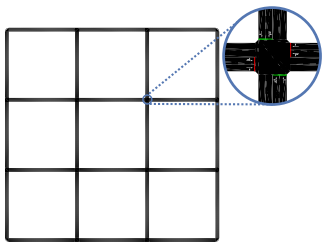

Fig. 4: Traffic map generated in SUMO.

C. Performance Evaluation

Starting from the basic scenario, we increase the number of vehicles from 70 to 100, in steps of 10. This allows us to investigate network performance over a range of different density scenarios. Since our aim is to investigate the performance of SAFERACO in both normal and sophisticated environments, we simulate two attacks: the black hole and flooding attacks. AntHocNet is chosen for comparisons in different scenarios. The average number of neighbors per vehicle should increase as the vehicle density gets higher. In consequence, more alternative routes should exist between source and destination vehicles. In general, alternative routes improve the reliability of routing protocol against link breakages. For example, if a link which is involved in an active route breaks, the routing protocol could directly choose an alternative route and continue the data transmission. This increases the PDR. However, due to the high vehicle density, there may exist more packet collisions which could lead to higher delay and overhead.

1) Performance under single attack: In this session, we compare SAFERACO with AntHocNet under single, separate

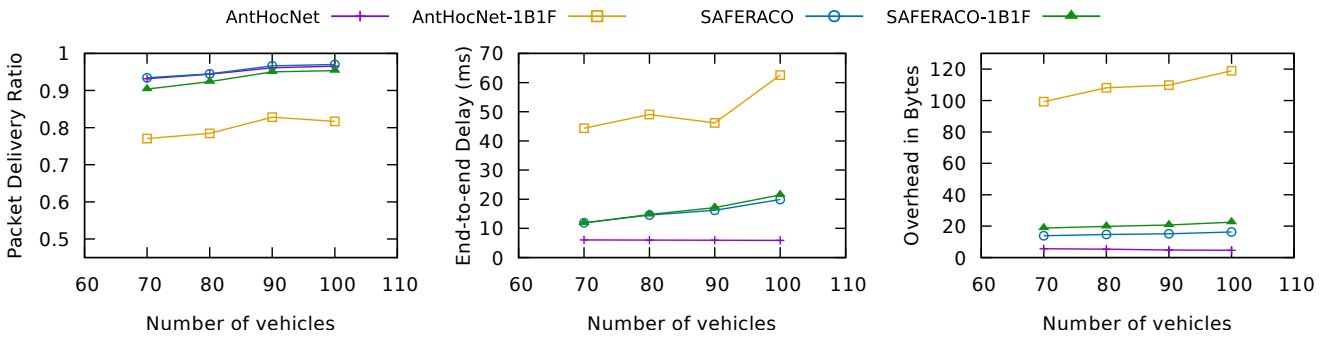

Fig. 5: Comparisons in multiple attacks scenarios.

attack. The simulation results for SAFERACO and AntHocNet in three different scenarios each are shown in Figure 3. It is clearly visible that the PDR increases with the vehicle density in all cases. In the scenario without any attacks, the PDR of these both protocols is very close. However, if there is one malicious node in the network, no matter it is a black hole node or flooding node, the PDR of SAFERACO-1B (1B means one black hole node) and SAFERACO-1F (1F means one flooding node) turns to be noticeably higher. The PDR of AntHocNet suffers more when under the black hole attack, while the PDR of SAFERACO under both black hole and flooding attacks remains almost the same as the case without any attacks.

The average end-to-end delay is also given in Figure 3. An increasing trend can be clearly recognized in both SAFERACO and AntHocNet when the network is attacked. The delay of AntHocNet-1F is the highest in all cases. This indicates that the delay of AntHocNet suffers the most under the flooding attack. In normal cases, the delay of both SAFERACO and AntHocNet are stable. However, the delay value drops very slightly under black hole attack in SAFERACO-1B and AntHocNet-1B. This is mainly an artifact of how delay is calculated in our experiments, where the delay caused by dropped packets is not considered. By looking to the PDR, we can see that SAFERACO-1B and AntHocNet-1B lost more data packets than the normal cases.

Figure 3 also presents the average overhead for the six cases. With growing density a moderate growth of overhead can be found in all cases. The overhead of AntHocNet-1F is obviously the highest one. This is mainly because of the flooded fake forward ant packets and other control packets caused by these fake forward ant packets. Other than AntHocNet-1F, the overhead of all cases is stable and the overhead of the three SAFERACO cases is higher than AntHocNet and AntHocNet-1B. This is due to false positives of the fuzzy detection system. The system cannot differentiate packets dropped due to black hole attacks and those packets dropped due to regular channel issues, such as packet collisions. Once a normal node is detected as a malicious node, it will not be selected in any routes until it has proven its benignity. This can cause a new route discovery process, which leads to additional overhead.

From the results we can observe that AntHocNet's PDR suffers a lot from the black hole attack and its delay and overhead suffers from the flooding attack. When using the AntHocNet routing protocol, either a black hole or a flooding node can attack the network routing process very effectively. In contrast, the performance of SAFERACO is stable under both attack. It does have higher delay or overhead in some cases, but its PDR is always better than that of AntHocNet when under attacks. This indicates that SAFERACO is robust, especially under black hole and flooding attacks. PDR, delay and overhead all increase with growing vehicle density.

2) Performance under combined attacks: In this section, we focus on comparing the performance of SAFERACO and AntHocNet under normal conditions as well as under multiple attacks at the same time. In multiple attack scenarios, there is a black hole node and a flooding node in the network at the same time (noted as 1B1F). These two malicious nodes work independently and do not collude with each other.

The simulation results for the protocols' performance are presented in Figure 5. Comparing the PDR of SAFERACO with SAFERACO-1B1F, we can see a slight drop between the two lines. This corresponds to the effectiveness of the black hole attack. However, the drop between AntHocNet and AntHocNet-1B1F is much more pronounced, showing its lower resilience against black hole attacks. The average end-to-end delay in Figure 5 shows that AntHocNet-1B1F has the highest delay which is similar to the case in Figure 3. This is mainly caused by the flooding attack. The delay of SAFERACO in both cases is higher than that of AntHocNet, with the same reason mentioned in section IV-C1. The average overhead is also shown in Figure 5. A moderate growth of overhead can be found in all four cases. Here, the overhead of AntHocNet-1B1F is obviously higher than in all other cases. Generally, the tendency in

Figure 5 is the same as the one in Figure 3. Looking at the differences in PDR over varying vehicle density, we find that high densities bring result in an increase in PDR. The same trend can be also found in the average end-to-end delay and the average overhead. However, there are some small differences. For example, the average delay of AntHocNet-1B1F is lower than that of AntHocNet-1F. This is mainly because the black hole attack caused a higher number of packets to be dropped and the delay of these dropped packets is not included in the calculation of the average delay. Moreover, the average overhead of AntHocNet-1B1F is higher than that of AntHocNet-1F in Figure 3. This indicates that both the black hole and flooding attack can lead to higher overhead in AntHocNet. Nevertheless, the difference between the SAFERACO-1B1F and SAFERACO-1F is very small. This indicates that SAFERACO is resilient against black hole and flooding attacks and that this resilience still keeps increasing with increasing vehicle density.

Overall, the PDR of SAFERACO is more stable and resilient against black hole attacks than that of AntHocNet and SAFERACO outperforms AntHocNet in delay and overhead when under flooding attacks.

V. Conclusion and Future Works

In this paper, we have proposed a security aware fuzzy logic enhanced reliable ant colony optimization based routing protocol for VANETs. SAFERACO is based on the AntHocNet routing mechanism and applies a distributed fuzzy logic detection system to exclude malicious nodes from the routing process. Thanks to its hybrid design, SAFERACO can discover optimal routes for efficient package delivery and, at the same itme, dynamically update the reliability ratings of nodes. The applied detection system robustly evaluates nodes based on limited information and has built-in high fault tolerance. Since the fuzzy reliability value will be updated dynamically, normal nodes which are misclassified as malicious nodes have a chance to prove their benignity by stably forwarding data packets. The results of various experiments show that, SAFERACO can efficiently protect the network from multiple attacks and is more stable and resilient against black hole and flooding attack than AntHocNet. For the future, we will further investigate the scalability of SAFERACO in different scenarios and a mechanism to dynamically adjust our fuzzy detection system on the spot will be considered. In order to better show that our approach is practical, we will also generate scenarios based on real maps. Another research direction is to evaluate the performance under different of attacks, such as Sybil and imposter attacks and to investigate further parameters that can be used as inputs for our fuzzy detection system to detect other types of attacks.

Acknowledgment

The authors would like to thank Leon Arian Tan for his very helpful contribution during the technical implementation.

References

[1] G. Carneiro, "NS-3: Network simulator 3," in *UTM Lab Meeting April*, vol. 20, 2010.

[2] H. Deng, W. Li, and D. P. Agrawal, "Routing security in wireless ad hoc networks," *IEEE Communications magazine*, vol. 40, no. 10, pp. 70–75, 2002.

[3] G. Di Caro, F. Ducatelle, and L. M. Gambardella, "AntHocNet: an adaptive nature-inspired algorithm for routing in mobile ad hoc networks," *European Transactions on Telecommunications*, vol. 16, no. 5, pp. 443–455, 2005.

[4] M. Dorigo and T. Stützle, *Ant Colony Optimization*. MIT Press, Cambridge, 2004.

[5] F. Ducatelle, "Adaptive routing in ad hoc wireless multi-hop networks," Ph.D. dissertation, Università della Svizzera italiana, 2007.

[6] H. T. Friis, "A note on a simple transmission formula," *Proceedings of the IRE*, vol. 34, no. 5, pp. 254–256, 1946.

[7] D. B. Johnson, D. A. Maltz, J. Broch *et al.*, "DSR: The dynamic source routing protocol for multi-hop wireless ad hoc networks," *Ad hoc networking*, vol. 5, pp. 139–172, 2001.

[8] B. Karp and H.-T. Kung, "Gpsr: Greedy perimeter stateless routing for wireless networks," in *Proceedings of the 6th annual international conference on Mobile computing and networking*. ACM, 2000, pp. 243–254.

[9] G. Korkmaz, E. Ekici, F. Özgüner, and Ü. Özgüner, "Urban multi-hop broadcast protocol for inter-vehicle communication systems," in *Proceedings of the 1st ACM international workshop on Vehicular ad hoc networks*. ACM, 2004, pp. 76–85.

[10] D. Krajzewicz, J. Erdmann, M. Behrisch, and L. Bieker, "Recent development and applications of sumo-simulation of urban mobility," *International Journal On Advances in Systems and Measurements*, vol. 5, no. 3&4, 2012.

[11] F. Li and Y. Wang, "Routing in vehicular ad hoc networks: A survey," *IEEE Vehicular technology magazine*, vol. 2, no. 2, 2007.

[12] J. P. Macker and M. S. Corson, "Mobile ad hoc networks (manets): Routing technology for dynamic wireless networking," *Mobile Ad hoc networking*, vol. 9, pp. 255–273, 2004.

[13] C. Maihofer, "A survey of geocast routing protocols," *IEEE Communications Surveys & Tutorials*, vol. 6, no. 2, 2004.

[14] C. Perkins, E. Belding-Royer, and S. Das, "Ad hoc on-demand distance vector (AODV) routing," Tech. Rep., 2003.

[15] R. Santos, R. M. Edwards, A. Edwards, and D. Belis, "A novel cluster-based location routing algorithm for inter-vehicular communication," in *Personal, Indoor and Mobile Radio Communications, 2004. PIMRC 2004. 15th IEEE International Symposium on*, vol. 2. IEEE, 2004, pp. 1032–1036.

[16] E. M. Shakshuki, N. Kang, and T. R. Sheltami, "Eaacka secure intrusion-detection system for manets," *IEEE transactions on industrial electronics*, vol. 60, no. 3, pp. 1089–1098, 2013.

[17] P. Yi, Z. Dai, S. Zhang, Y. Zhong *et al.*, "A new routing attack in mobile ad hoc networks," *International Journal of Information Technology*, vol. 11, no. 2, pp. 83–94, 2005.

[18] S. Zeadally, R. Hunt, Y.-S. Chen, A. Irwin, and A. Hassan, "Vehicular ad hoc networks (vanets): status, results, and challenges," *Telecommunication Systems*, vol. 50, no. 4, pp. 217–241, 2012.

[19] H. Zhang, A. Bochem, X. Sun, and D. Hogrefe, "Employing fuzzy logic to provide security awareness in aco routing for manets," in *proceedings of the IEEE Wireless Communications and Networking Conference*. IEEE, 2018.

[20] H. Zhang, X. Wang, P. Memarmoshrefi, and D. Hogrefe, "A survey of ant colony optimization based routing protocols for mobile ad hoc networks," *IEEE Access*, vol. 5, pp. 24 139–24 161, 2017.