A Security Aware Fuzzy Enhanced Ant Colony Optimization Routing in Mobile 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}@informatik.uni-goettingen.de
xu.sun@stud.uni-goettingen.de

***Abstract*—As mobile ad hoc networks (MANETs) grow more popular and are deployed as solutions in various applications such as road safety (vehicular networks), wildlife tracking (wireless sensor networks) and device-to-device communications in 5G, the need for efficient routing that is robust against malfunctioning or malicious network nodes is increasing. We propose a security aware fuzzy enhanced ant colony optimization (SAFEACO) routing algorithm, which makes use of a fuzzy logic module to identify misbehaving nodes and exclude them from the routing process. We evaluate the SAFEACO routing algorithm, by comparing it with another modern and widely known approach and found that it shows superior performance in all relevant metrics, such as packet delivery ratio, delay and overhead. Due to its ability to identify misbehaving nodes, SAFEACO also provides a higher level of robustness against black hole and Sybil attacks.**

***Index Terms*—Security, Ant Colony Optimization, Fuzzy Logic, Routing, MANETs**

I. Introduction

Over time the relevance of mobile ad hoc networks (MANETs) [13] has grown and different types of MANETs become increasingly more widespread and larger in scale. For example, vehicular ad hoc networks (VANETs) [20] allow vehicles to coordinate while in traffic, improving road safety and efficiency. Wireless sensor networks (WSNs) [16] are used to track various types of environmental data, both in stationary and mobile scenarios, such as wildlife tracking. 5G [2] mobile communications include the concept of device-to-device (D2D) [9] communication which is in effect forming MANETs between cellular phones and other mobile terminals, necessitating improved efficiency in wireless routing. The ant colony optimization (ACO) algorithm [6] has shown the ability to efficiently find optimal routes in MANETs, while also being able to adapt to the constantly changing topology of such 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 just as well in networks as it does in nature.

As the value of these networks increases the motivation of attackers to manipulate or disrupt them also increases. Therefore, the growing popularity and prevalence of MANETs necessitates effective and efficient routing methods that are also robust against malfunctioning devices and malicious network participants. One concrete example for the benefit MANETs can bring to humanity, which also highlights the importance of its security awareness, is the helpfulness of MANETs in search and rescue operations. In these, MANETs can be deployed in areas with little or no wireless infrastructure support, such as in disaster relief situations. However, in such environments, human life can be endangered if the network is not operating correctly due to attacks.

In this paper, we propose a security aware fuzzy enhanced ant colony optimization (SAFEACO) based routing protocol for MANETs which employs a fuzzy logic module to evaluate the behavior of nodes in the network. Fuzzy logic is well suited in situations, where network participants cannot be unambiguously assigned to either the class of reliable or unreliable nodes, because it allows the representation of partial memberships in different classes. Our approach assigns reliability scores and is able to exclude non-benign nodes from the routing process. The evaluation of SAFEACO shows its effectiveness in both routing and protecting the network from attacks.

This paper is organized in the following way: Section II reviews related work. Our routing methodology is described in detail in Section III. Section IV provides a detailed evaluation of our approach. Finally, we give our conclusions and point out future ways of enhancement in Section V.

II. Related Work

Over the past two decades, researchers have proposed various routing approaches, such as Ad hoc On-Demand Distance Vector routing (AODV) [15], Dynamic Source Routing (DSR) [11]. In the early development phase of MANETs, these protocols were considered to be state of the art protocols and were sufficient to satisfy the demands of MANET applications. However, more and more advanced applications required increasingly higher levels of sophistication from these protocols. This encourages researchers to design new routing protocols, which could provide higher packet delivery ratio, lower end-to-end delay and less overhead, while also providing high levels of security.

The ACO algorithm presents a common framework for approximating solutions to NP-hard optimization problems [6]. Due to the dynamic nature of ACO's connectivity, ACO is able to continuously adapt to network changes in real time [1]. Moreover, the artificial ants can find multiple solutions

simultaneously for the considered problem [6]. Therefore, ACO based algorithms are able to efficiently find optimal routes, which has lead to applying them in the field of routing for network communication. AntHocNet[5] is a representative hybrid ACO based routing protocol, in which reactive ants are used to discover new routes, while proactive ants are used to explore alternative routes during data transfer sessions. However, security in AntHocNet remains an open issue.

FTAR [17] is the fuzzy-based trusted ant routing protocol which combines the ACO algorithm with a fuzzy system to select optimal routes. FTAR aims to distinguish between healthy and malicious nodes. However, the authors neither explain how they obtain the input parameters for their fuzzy control system, nor do they give a detailed explanation of how to use the fuzzy based trust value in the ACO routing structure. Due to these reasons, we could not re-implement their work and compare its performance with ours.

EAACK which was proposed by Shakshuki et al. [18] in 2013 is one of the widely cited approaches in the recent five years. It is based on the DSR [11] protocol and employs an enhanced adaptive acknowledgment scheme to detect malicious nodes. However, the authors do not evaluate the end to end delay of EAACK. Since EAACK is based on DSR, its reactive routing mechanism should lead to a higher amount of delay than would be present in a hybrid scheme. Due to certain properties, in highly dynamic networks, delay can increase even further when routing issues occur.

III. SAFEACO Routing in MANETs

The aim of SAFEACO is to design a routing protocol in MANETs which can provide a high packet delivery ratio, low end-to-end delay and low communication overhead in normal scenarios as well as in attack scenarios. Therefore, SAFEACO has to guarantee both efficiency and security. In this section we first introduce the hybrid routing mechanism of SAFEACO. The attack models implemented in this work are presented afterwards. Finally, we explain how the fuzzy enhanced detection system works as a part of the SAFEACO routing process.

A. Reactive Route Setup in SAFEACO

In order to apply the ACO algorithm to the problem of routing in MANETs, the network is represented as a graph [3]. Figure 1 shows an example, where an optimal route between the nodes S and D should be found. Ants can only travel along the edges of the graph, which represent the communication links between the nodes participating in the network.

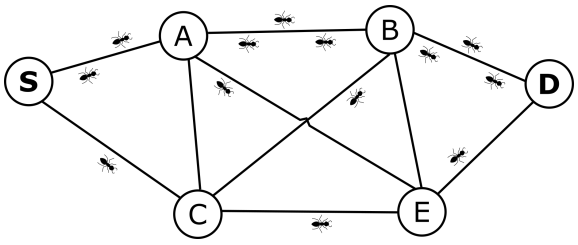


Fig. 1: An example while applying ACO meta-heuristic.

To find a route, node S broadcasts reactive forward ants (FANT)s. The probability for a reactive FANT which starts from node i to choose node j as the next hop is defined as in equation 1.

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

$P_{ij}^{d}(t)$ is the probability of an ant moving from node i to node j on the way to the destination node d at the t-th iteration step or time slot; N_i^d is the set of current neighboring nodes of node i; $\tau_{ij}^{d}(t)$ is the regular pheromone value on the link between nodes i and j on the way to destination node d at t-th iteration step or time slot; $R_{ij}(t)$ is the reliability value estimated by the fuzzy detection system for the link between nodes i and j at the t-th iteration step or time slot; $\alpha \geqslant 1$, is a parameter which controls the exploratory behavior of the ants.

A reactive FANT moves hop by hop until it reaches the destination node or until the maximum travel hop count of the ant is reached. For each step, it chooses one of its neighbor nodes according to Equation 1. After the ant arrives at the destination node, it turns into a backward ant (BANT) and travels back to the source node by following exactly the same route. At each intermediate node, 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 node i to node d along this route. The amount of pheromone updates assigned to a link is calculated based on the quality of the route and the pheromone evaporation rate, as shown in Equation 2. An ant considers the quality of a route to be an amount that is 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 nodes i and j; τ_{ij}^{new} is the updated regular pheromone value; $\rho \in (0, 1]$ is the pheromone evaporation rate. 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 of for the SNR, at which a link is considered to be bad; C_{const} is the cost of using a bad link.

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 the Equation 1.

B. Proactive Route Maintenance in SAFEACO

The proactive route maintenance mechanism in SAFEACO consists of two parts: pheromone diffusion and proactive ant sampling.

1) Pheromone diffusion: In this process, node i, chooses randomly up to 10 destinations to which it has valid routing information. It makes a list of these destinations, their corresponding best pheromone values and a flag that shows whether the best pheromone is a regular pheromone value or a virtual pheromone value for the route. Node i adds this list to its hello message and broadcasts it regularly to all neighbor nodes. After receiving a hello message from node i, the neighbor node j, checks the routing information in the hello message. For each reported destination node in the list, node j estimates separately a virtual pheromone value ω_{ji}^d from itself to this destination node d in the way as shown in Equation 4.

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

V_i^d is the reported pheromone value of this route, which indicates the quality of the best route from node i to node d; C_j^i is the locally maintained cost value of hopping from node j to node i.

2) Proactive ant sampling: In this process, source nodes send out proactive forward ants regularly during data sessions. Proactive forward ant apply a probability rule described in Equation 5 to choose their next hop.

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

Once the proactive ant reaches its destination node, it is converted into a proactive backward ant which has the same behavior of a 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 attractive 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.

In order to ensure fairness for the comparison in section IV, all the weight and threshold values in the routing process use the same values as in AntHocNet's implementation [8].

C. Attack Models

In order to investigate the performance of SAFEACO under different attacks, we implemented two attack models in our experiments.

1) Black hole attack: Since packet-dropping attacks are a major threat to the security of MANETs [18], in this work we choose the black hole attack introduced in [4] as one of the attack models to investigate SAFEACO's performance. In this attack model, as soon as black hole node M receives a FANT, it replies the source node immediately with a BANT in 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.

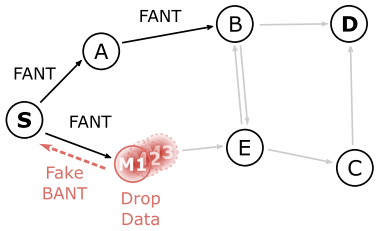


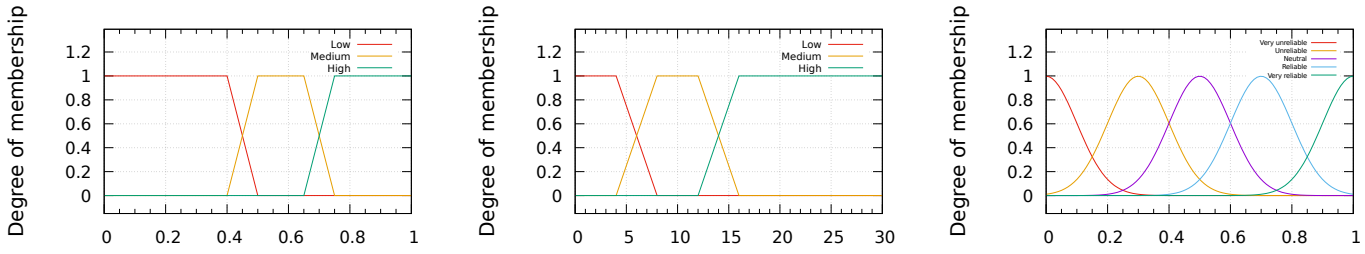
Fig. 2: Sybil with black hole attack model.

2) Sybil attack: In 2002 J. R. Douceur first introduced the Sybil attack [7] in context of peer-to-peer networks. In the Sybil attack, a malicious node presents multiple identities to the other nodes in the network. C. Karlof and D. Wagner pointed out that the Sybil attack can threaten the routing mechanism in wireless sensor networks [12]. J. Newsome et al. established a classification of different kinds of the Sybil attack in [14]. According to this classification, Sybil attacks can be divided into simultaneous and Non-Simultaneous attacks.

In our experiments, we implemented a special case of the Non-Simultaneous Sybil attack. A Sybil node in our experiments has multiple (at least two) Sybil identities. Every Sybil identity is not duplicated with any other nodes' identity in the network. Sybil node presents only one of its identities to the network at a time, but it switches its identity in a predefined interval. However, if the Sybil node only switch its identities in the routing process, it doesn't affect much the routing performance. In order to better understand the effects made by the Sybil attack, we combine the Sybil and black hole attack together. We let each Sybil identity launch the black hole attack. Figure 2 shows that a Sybil node M which has three identities: M1, M2 and M3, in the network. In every 50 seconds, node M switches its identity and it uses the current identity to launch the black hole attack until the next switch moment.

D. Fuzzy Logic Based Detection System

SAFEACO applies a distributed fuzzy logic based malicious behavior detection system based on a traffic monitoring system to isolate the malicious nodes. Due to their inherent mobility, usually only very limited information about its surrounding environment is available to a node. 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 it 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.



(a) Forward rate (b) Recent transmission (c) Reliability

Fig. 3: Membership functions for inputs (3a, 3b) and output (3c).

The *forward rate* is the ratio of packets forwarded by a node to packets sent to a node. The *recent transmission* is defined as the number of packets sent to a given node for forwarding. In the fuzzy system, these two input values can either be ”low”, ”medium” or ”high”. Their membership functions are given in Figure 3a and Figure 3b respectively. The output value is called *reliability*. It represents the quality of the link and is employed to make decisions regarding the routing process. This output value can be either ”very unreliable”, ”unreliable”, ”neutral”, ”reliable” or ”very reliable”. Its membership function is given in Figure 3c. As shown in Figure 4, the input values are first fuzzified. Then, the system performs the inferencing based on a number of predefined rules and the membership functions and give the results to the defuzzifier. Finally, the defuzzifier outputs the *reliability* value. The rule base used for inference is described in Table I. In this table, a vector (L, M) means, that the *forward rate* is has value L and the *recent transmission* has value M. The possible values are **L**ow, **M**edium and **H**igh. In our experiments, we set the threshold value of this value to 0.12. All nodes whose reliability value is below the threshold value are considered unreliable and will not be chosen by reactive or proactive forward ants.

Since the traffic monitoring system only observers traffic in the network, the detection system does not cause any additional control packets in the routing protocol. In SAFEACO, every node monitors each of its neighbor nodes' behaviors and passes the observed parameters, namely the forward rate and the number of recent transmissions of packets to be forwarded, into its fuzzy inference system. The fuzzy inference system estimates the reliability value of the observed neighbor node.

In this work, we chose the forward rate and the number of recent transmissions of packets to be forwarded to detect black hole attacks. If other attacks against routing protocols should also be considered, e.g. flooding attacks, we can add additional inputs to our fuzzy detection system, which can for example reflect the route request sending frequency of a neighbor node. We can then add adapted, new fuzzy rules into 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.

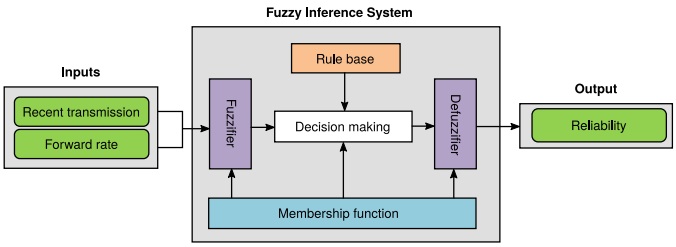


Fig. 4: Block diagram of SAFEACO's fuzzy module.

Reliability	Input combinations
Very reliable	(H, H), (H, M)
Reliable	(H, L), (M, L)
Neutral	(L, L), (M, M)
Unreliable	(M, H)
Very unreliable	(L, M), (L, H)

TABLE I: Applied fuzzy rules.

IV. Evaluation

In order to investigate the performance of SAFEACO when undergoing black hole attacks, we have implemented the proposed approach in the NS-3 simulator and compared its performance to that of EAACKm, which is based on EAACK [18], but was modified slightly to ease implementation without negatively impacting performance under the given scenario.

A. Evaluation Measures

1) Packet Delivery Ratio (PDR): This parameter is calculated by using 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 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 amount of time that passes between its sending and receiving time. For each simulation run, this value is 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. 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 problem it has been designed to address. Having a high PDR and a low delay measure with low or reasonable overhead would show that SAFEACO is suitable as a routing algorithm in general. To collect the data, we performed ten runs of the simulation for each scenario with different random seeds and averaged the results.

B. Basic Scenario

In the basic scenario, there are 50 nodes in a rectangular area with dimensions of $500\,\mathrm{m} \times 1500\,\mathrm{m}$. It's assumed that the area is completely free of obstacles which could affect the nodes' movement or radio transmissions. Node mobility is modeled according to a modified random waypoint model (RWP) with a minimum speed to mitigate the known issues [19] with this model. The nodes move with a randomly selected speed between $5\,\mathrm{m/s}$ and $20\,\mathrm{m/s}$ and the pause time is set to $30\,\mathrm{s}$. Radio transmission is modeled according to the Friis propagation model [10], with a transmission range of approximately $250\,\mathrm{m}$. 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 $900\,\mathrm{s}$.

C. Performance Evaluation Under Black Hole Attacks

Starting from the basic scenario, we vary the maximum speed of the nodes between $5\,\mathrm{m/s}$ and $30\,\mathrm{m/s}$ in $5\,\mathrm{m/s}$ steps. AODV, AntHocNet and EAACKm are chosen for comparisons in different scenarios. The abbreviations used in our figures can be found in Table II.

In theory, the topology of the network changes more frequently as the mobility of nodes increases. In consequence, links break more often than in a network with low mobility nodes. Generally speaking, link breakages lead to more overhead, lower PDR and higher delay. For example, if a link which is involved in an active route breaks, the routing protocol should react to this change. Normally route error messages are sent out which causes more overhead and may cause intermediate nodes to try and find an alternative route to salvage the data packets affected by the link breakage. If the intermediate nodes successfully find a new route, they can forward the buffered data packets to the destination nodes; otherwise, the buffered packets will be dropped. This leads to a lower PDR. The salvaged data packets also cause a higher delay, due to the buffer time at the intermediate nodes.

Abbreviation	Description
AODV-0BH	AODV without black hole
AntHocNet-2BH	AntHocNet with 2 black holes
EEACKm-0BH	EEACKm without black hole
EEACKm-2BH	EEACKm with 2 black holes
SAFEACO-0BH	SAFEACO without black hole
SAFEACO-2BH	SAFEACO with 2 black holes

TABLE II: Abbreviations of different configurations.

Figure 5 shows that the increasing node speed doesn't affect the Packet Delivery Ratio (PDR) strongly. In most of the cases, PDR remains in a similar level. One exception is the PDR of EAACKm-0BH dropping obviously when node speed increases. This indicates that EAACKm suffers more by the high mobility. In the scenario without any attacks, AntHocNet shows the best PDR and SAFEACO with a slightly lower PDR is at the second place. It is claerly better than EAACKm and AODV. However, if there are black hole nodes in the network, AntHocNet suffers more than the other two security aware protocols and SAFEACO turns out to be the best solution. An increasing trend in the average end-to-end delay can be clearly recognized in both SAFEACO and EAACKm. The delay of EAACKm is obviously higher than the one of SAFEACO in all cases. Although AntHocNet has the lowest delay, this is mainly an artifact of how delay is calculated in our experiments, where the delay caused by dropped packets is not considered. A moderate growth of overhead can be found for all protocols in Figure 5. The overhead of SAFEACO and EAACKm is almost at the same level.

D. Performance Evaluation Under Sybil Attacks

From the base scenario, we keep all parameters the same except for setting one node in the network to be the Sybil node which has two identities that are switched in every 50 seconds. The Sybil node launches black hole attack with each of its identities. Figure 6 shows that the PDR of both protocols decreases when the number of Sybil nodes increases from 1 to 10. However, the PDR of SAFEACO is obviously higher than that of EAACKm. SAFEACO can deliver almost $70\,\%$ of the data packets even when $20\,\%$ of the network size are malicious, while EAACKm can only deliver about $30\,\%$ of the data packets under the same conditions. The end to end delay of both protocols decreases when the number of Sybil nodes in the network increases. This tendency is probably due to the way how delay is calculated, in which the dropped data packets are not considered. From the PDR Figure we can observe that the percentage of dropped data packets is getting higher when the number of Sybil nodes is increases. A moderate increasing trend in the average overhead in bytes for SAFEACO is shown in the figure. However, the overhead of SAFEACO is still lower than that of EAACKm. The results indicate that SAFEACO shows clearly better performance and robustness in comparison with EAACKm when under Sybil attacks.

V. Conclusion and Future Works

In this paper, we have proposed a security aware fuzzy logic enhanced ant colony optimization based routing protocol for MANETs. SAFEACO is able to efficiently deliver the packets while dynamically detecting the malicious nodes in the

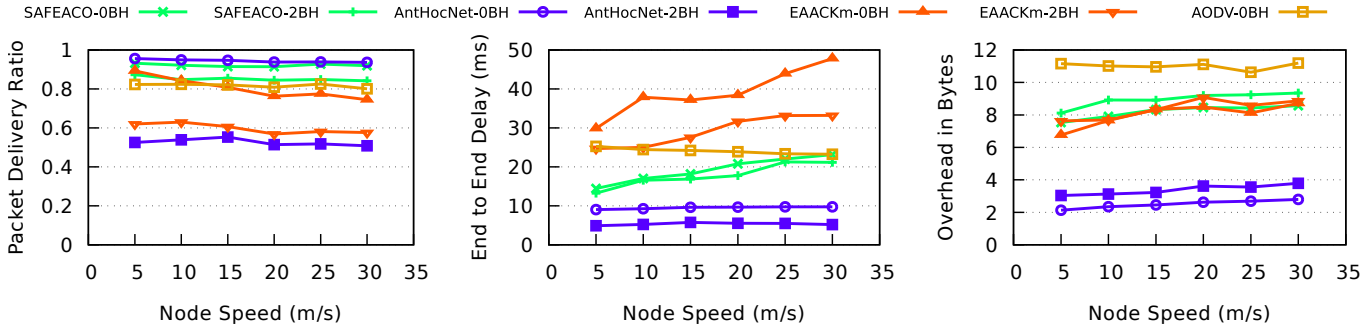


Fig. 5: Average values over varying node speed.

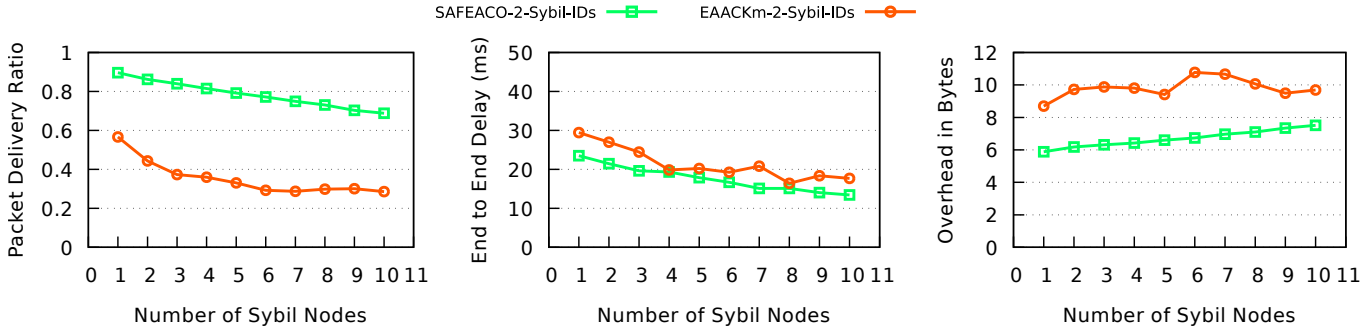


Fig. 6: Average values over varying Sybil node number.

network. The fuzzy based detection system robustly evaluates nodes based on limited information and has built-in high fault tolerance. The results of varying the node speed experiments show that, the PDR performance of SAFEACO remains almost in the same level as the node speed increases. Specially, in comparison with other protocols, SAFEACO has the best PDR performance under black hole attacks. Moreover, SAFEACO also shows clearly better performance and robustness with its higher PDR and lower delay and overhead than EAACKm in scenarios with Sybil nodes. For the future, we will further investigate the scalability of SAFEACO in different scenarios, such as varying the node density, increasing data send rate, and so on. Since our fuzzy based detection system is able to detect different types of attacks, we will investigate new input parameters for the fuzzy system to protect the network from other types of attacks.

References

[1] H. Ahmed and J. Glasgow, "Swarm intelligence: concepts, models and applications," *School Of Computing, Queens University Technical Report*, 2012.

[2] J. G. Andrews, S. Buzzi, W. Choi, S. V. Hanly, A. Lozano, A. C. Soong, and J. C. Zhang, "What will 5g be?" *IEEE Journal on selected areas in communications*, vol. 32, no. 6, pp. 1065–1082, 2014.

[3] D. W. Corne, A. Reynolds, and E. Bonabeau, "Swarm intelligence," in *Handbook of Natural Computing*. Springer, 2012, pp. 1599–1622.

[4] 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.

[5] 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.

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

[7] J. R. Douceur, "The sybil attack," in *International workshop on peer-to-peer systems*. Springer, 2002, pp. 251–260.

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

[9] D. Feng, L. Lu, Y. Yuan-Wu, G. Y. Li, G. Feng, and S. Li, "Device-to-device communications underlaying cellular networks," *IEEE Transactions on Communications*, vol. 61, no. 8, pp. 3541–3551, 2013.

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

[11] 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.

[12] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures," *Ad hoc networks*, vol. 1, no. 2-3, pp. 293–315, 2003.

[13] 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.

[14] J. Newsome, E. Shi, D. Song, and A. Perrig, "The sybil attack in sensor networks: analysis & defenses," in *Proceedings of the 3rd international symposium on Information processing in sensor networks*. ACM, 2004, pp. 259–268.

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

[16] C. S. Raghavendra, K. M. Sivalingam, and T. Znati, *Wireless sensor networks*. Springer, 2006.

[17] S. Sethi and S. K. Udgata, "Fuzzy-based trusted ant routing (FTAR) protocol in mobile ad hoc networks," in *International Workshop on Multi-disciplinary Trends in Artificial Intelligence*. Springer, 2011, pp. 112–123.

[18] 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.

[19] J. Yoon, M. Liu, and B. Noble, "Random waypoint considered harmful," in *INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies*, vol. 2, March 2003, pp. 1312–1321 vol.2.

[20] 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.