

**Packet-Dropping and False-Recommendation Attacks on Trust-Based Gateway
Selection in an Integrated Internet-MANET: An NS-3 Study**Mohammed Abdul Raheem¹, Khaleel Ur Rahman Khan²¹Research Scholar, Rayalaseema University, Kurnool, Andhra Pradesh, India (maraheem@mjccollege.ac.in)²ACE Engineering College, Hyderabad, Telangana, India (khaleelrkhan@gmail.com)

Abstract—In an integrated Internet-MANET a mobile node reaches the Internet through a gateway, and the choice of gateway decides which relay nodes carry its traffic. If some of these relays accept packets and then discard them, the choice of the nearest gateway is no longer the safest one. This paper studies a trust-based gateway selection in the ns-3 simulator. A watchdog based on overheard transmissions supplies evidence, the Beta expectation turns it into trust, and a source switches to another gateway when the relays on its route to the current one are not trusted. Two gateways serve a 30-node AODV network in which 0, 10, 20 and 30 per cent of the nodes drop every packet they should relay; every setting was run ten times. Compared with selecting the nearest gateway, trust-aware selection lowered the share of selections whose route contained a dropping relay from 5.9 to 3.6 per cent at 30 per cent dropping nodes and raised the packet delivery ratio from 0.922 to 0.936, at the price of about seven additional gateway switches per flow. The trust values themselves were reliable only while the opinions of other nodes were honest: when the dropping nodes also sent false opinions, mean and median aggregation condemned 55 and 43 per cent of the honest nodes at 10 per cent attackers, whereas weighting the opinions by the trust of their sender removed the effect. The results show that a trust-aware gateway choice gives a small but consistent gain in an attack-prone network, and that the treatment of recommenders decides whether the trust values can be used at all.

Keywords—Integrated Internet-MANET, gateway discovery, trust management, watchdog, blackhole, false recommendation, Beta reputation, ns-3

I. INTRODUCTION

A mobile ad hoc network (MANET) can be connected to the Internet through one or more gateways, which gives its nodes access to remote services while keeping the freedom of an infrastructure-less network. A node that wants to use the Internet first has to find a gateway and then send its packets over the multi-hop route to it. The mechanisms for finding gateways have been studied for many years; the main families are proactive advertisement, reactive solicitation and a hybrid of the two [1, 2]. Several adaptive versions adjust the advertisement range and the advertisement interval to the traffic and the mobility of the network [3, 4].

Almost all of this work assumes that the nodes on the route to a gateway forward the packets they are given. In an open network this assumption can fail. A relay may be selfish or compromised, may answer route requests so that it attracts traffic, and may then discard the data. Then the gateway that is nearest in hops is not necessarily the one that delivers the most packets, because the route to it may pass through a node that drops. A source that can judge its relays could prefer a longer but trusted route to the other gateway.

Trust management provides the means for this judgement [5]. The watchdog of Marti et al. [6] lets a node observe whether the neighbour to which it handed a packet transmits the packet again, and a reputation formula such as the Beta system [7] converts the observations into a trust value. The weak point of such schemes is the exchange of opinions, since a node that misbehaves can also send false opinions [8, 9]. This paper takes the view that gateway discovery in an integrated Internet-MANET should be trust based and adaptive, and evaluates one concrete piece of that idea: the selection of the gateway by a source node from the trust of the relays on the routes to the available gateways.

The contributions of the paper are as follows. (1) A trust-based gateway selection algorithm that reads the actual AODV route to each gateway and combines the hop count with the weakest trust value along the route. (2) An ns-3 implementation, with a watchdog built on promiscuous reception, two gateways reached through UDP, and online trust values that are used by the selection while the simulation runs. (3) A paired comparison with nearest-gateway selection for 0, 10, 20 and 30 per cent of dropping nodes, with ten runs for each setting, measuring delivery, delay, exposure to dropping relays and the number of gateway switches. (4) An evaluation of mean, median and trust-weighted aggregation of opinions when the dropping nodes also send false opinions about honest nodes and about each other.

The paper is organised as follows. Section II gives the background and related work, Section III describes the system, the trust model and the algorithms, Section IV the simulation set-up, Section V the results, Section VI the limitations, and Section VII concludes.

Table 1. Notation

Symbol	Meaning
$r(i,j)$, $s(i,j)$	Decayed counts of packets that observer i saw forwarded / dropped by j
w, T_0	Weight and centre of the prior of the Beta expectation (initial trust)
λ	Forgetting factor applied at the end of every 5 s slot
$T(i,j)$, $T(j)$	Direct trust of i in j ; network-level trust of j
$\theta, n_{\min}$	Decision threshold (0.5); minimum number of observations (3)
$PT(g)$	Path trust of the route to gateway g ; the smallest $T(\cdot)$ among its relays

B. Watchdog evidence

When node i hands a data packet to a next hop j that is not the destination, i starts a watch on the packet. If i overhears j transmit the packet within 0.5 s, the packet is counted as forwarded; otherwise it is counted as dropped. The counts of each observer–suspect pair are collected in slots of 5 s (Algorithm 1). This evidence is imperfect: a relay whose route has just broken also discards the packet, and the watchdog cannot tell this case from a deliberate drop.

Algorithm 1. Watchdog evidence collection at observer i 1. Input: data packet handed by node i to next hop j (j is not the destination) 2. On hand-over: start watch timer $W = 0.5$ s; set $\text{pending}(i, j, \text{packet}) = \text{true}$ 3. On overhearing j transmit the same packet before W expires: 4. $\text{forwarded}(i, j, \text{slot}) += 1$; $\text{pending} = \text{false}$ 5. On W expiry with $\text{pending} = \text{true}$: 6. $\text{dropped}(i, j, \text{slot}) += 1$ 7. At the end of every 5 s slot k , report the pair (forwarded , dropped) for each j

C. Trust computation

For every observer i and suspect j the node keeps two decayed counters, $r(i,j)$ for forwarded and $s(i,j)$ for dropped packets. Trust is the Beta expectation with a prior of weight w centred on the initial trust T_0 :

$$T(i,j) = [r(i,j) + w \cdot T_0] / [r(i,j) + s(i,j) + w] \quad (1)$$

At the end of every slot the counters are multiplied by a forgetting factor λ before the new evidence is added. In this study $\lambda = 1$, $w = 2$ and $T_0 = 0.5$. The network-level trust $T(j)$ is the mean of $T(i,j)$ over the observers that hold at least three observations of j , and node j is regarded as misbehaving when $T(j) < \theta$ with $\theta = 0.5$ (Algorithm 2).

Algorithm 2. Beta trust update with forgetting factor and initial trust 1. Input: counters $r(i,j)$, $s(i,j)$; prior weight w ; initial trust T_0 ; forgetting factor λ ; slot evidence (f, d) 2. At the end of each slot: 3. $r(i,j) = \lambda \cdot r(i,j) + f$; $s(i,j) = \lambda \cdot s(i,j) + d$ 4. $n = r(i,j) + s(i,j)$ 5. $T(i,j) = (r(i,j) + w \cdot T_0) / (n + w)$ 6. Network trust of j : $T(j) = \text{mean of } T(i,j) \text{ over observers } i \text{ with } n \geq n_{\min} = 3$ 7. If no observer has $n \geq n_{\min}$ then $T(j) = T_0$ 8. Node j is trusted if $T(j) \geq \theta$, otherwise it is marked as misbehaving

D. Trust-aware gateway selection

Every 10 s each source reads the AODV routing tables along the route to each gateway and obtains the hop count and the relay nodes. The path trust PT of a route is the smallest network trust among its relays, so that one dropping relay is enough to make the route untrusted; a direct route has $PT = 1$. Among the routes with $PT \geq \theta$ the source takes the one with the fewest hops, and if there is none it takes the route with the highest PT (Algorithm 3 and Figure 2). The baseline policy chooses the gateway with the fewest hops, whatever the trust values are. Both policies keep the current gateway when the candidates are equal.

Algorithm 3. Trust-aware gateway selection by a source node 1. Input: gateways G , source s , threshold θ , period 10 s 2. Every 10 s, for each gateway g in G read the AODV route from s : 3. if there is no valid route then mark g as unreachable 4. $\text{hops}(g) = \text{number of hops}$; $R(g) = \text{relay nodes on the route}$ 5. $PT(g) = \min \text{ of } T(r) \text{ over } r \text{ in } R(g)$ ($PT(g) = 1$ for a direct route) 6. $T = \{ g \text{ reachable} : PT(g) \geq \theta \}$ 7. If T is not empty then choose g^* in T with the fewest hops (keep the current gateway on a tie) 8. Else choose the reachable g^* with the largest $PT(g)$ 9. If g differs from the current gateway then switch the flow to g

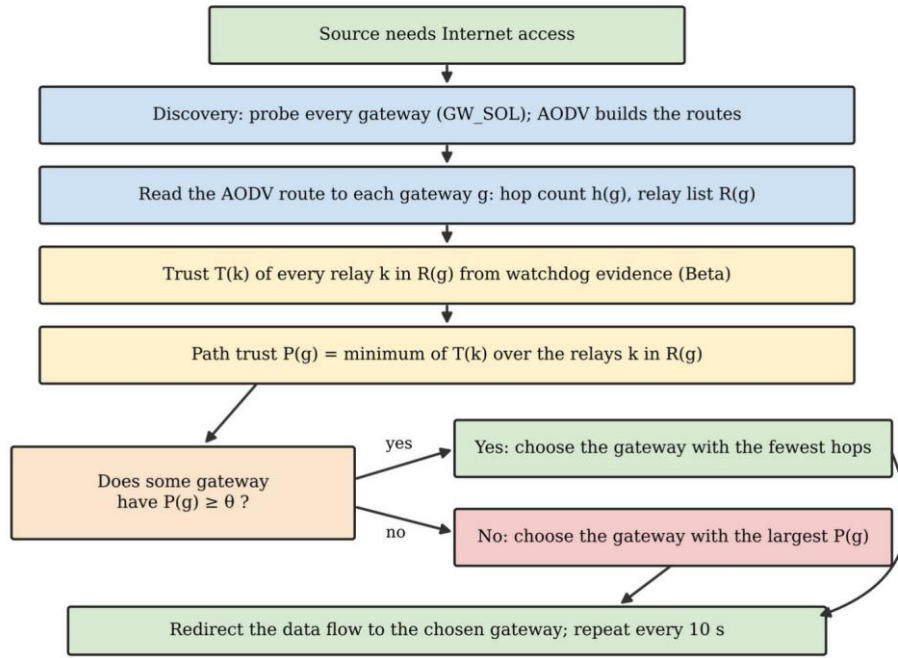


Figure 2. Flow of the trust-aware gateway selection.

E. Recommendations and the false-recommendation attack

When nodes exchange their trust values, the network trust of j is an aggregate of the reports about j . Three aggregations are compared: the mean, the median, and the trust-weighted mean in which the report of node k has the weight $T_0(k)$ if $T_0(k)$ exceeds θ and zero otherwise, where $T_0(k)$ is the trust of k computed from direct evidence alone (Algorithm 4). In the false-recommendation attack every dropping node reports 0 for each honest node (bad-mouthing) and 1 for each other dropping node (ballot stuffing), whether or not it has evidence.

Algorithm 4. Trust-weighted aggregation of recommendations 1. Input: reports $T(k, j)$ from nodes k ; direct network trust $T_0(k)$ of each reporter k 2. For every reporter k : $w(k) = T_0(k)$ if $T_0(k) > \theta$, otherwise $w(k) = 0$ 3. $T(j) = \sum_k w(k) \cdot T(k, j) / \sum_k w(k)$ 4. If $\sum_k w(k) = 0$ then $T(j) = T_0$ (no usable opinion) 5. Return $T(j)$ to the gateway selection algorithm

F. Overhead and complexity

The scheme adds three kinds of cost. First, the probes: each source sends a 20-byte packet to every gateway every 5 s, so the control traffic per flow is 4 B/s per gateway, which is small beside the 2 kB/s of the data flow of 512 B every 0.25 s. Second, the watchdog needs promiscuous reception and one timer per handed-over packet, which costs energy and memory at the relay and is the usual price of watchdog schemes [6]. Third, the selection reads the route table along the path, which in a real implementation would be replaced by a route record or by a field of the route reply, since a source normally knows only its own next hop. The cost of the evidence exchange (the reports of Algorithm 4) grows with the number of observed pairs, that is, quadratically in the worst case, and would need to be limited to neighbours and gateways in a large network.

IV. SIMULATION SET-UP

The simulations were run in ns-3.49 [20] with the parameters of Table 2. The 30 MANET nodes move with the random-waypoint model in an 800 m × 800 m area; two gateways are placed at fixed positions on the horizontal centre line, at one-third and two-thirds of the width, and the Internet side is represented by the gateways as data sinks. Twelve flows start at randomly selected honest nodes and send 512 B every 0.25 s to the gateway currently chosen by the source. In addition, each source sends a short probe to every gateway every 5 s so that AODV keeps a route to both, which corresponds to reactive discovery. The dropping nodes were drawn at random among the MANET nodes, and their IP forwarding was switched off, so that AODV still lets them take part in route discovery. The trust values used by the selection are computed online from the evidence of all honest observers, so they correspond to a truthful exchange of opinions; the false-recommendation attack is analysed on the recorded evidence offline. Every setting was repeated with ten seeds, and all values are means with the half-width of the 95 % confidence interval over the runs. For the comparison of the two policies the same seed was used for both, and the difference was tested with a paired t-test.

Table 2. Simulation parameters

Parameter	Value
Simulator / routing	ns-3.49 / AODV
MANET nodes / gateways	30 / 2 (fixed)
Area	800 m × 800 m
Radio range	250 m (range propagation model)
MAC / rate	IEEE 802.11g ad hoc, 6 Mb/s
Mobility	Random waypoint, 1–5 m/s
Traffic	12 CBR/UDP flows, 512 B every 0.25 s
Gateway re-selection period / probe period	10 s / 5 s
Simulation time	300 s
Dropping nodes	0, 3, 6, 9 (0, 10, 20, 30 %)
Watchdog timeout / slot	0.5 s / 5 s
Trust parameters	$T_0 = 0.5$, $w = 2$, $\lambda = 1$, $\theta = 0.5$, $n_{\min} = 3$
Policies	Nearest gateway; trust-aware
Runs per setting	10 seeds (9 for 0 %)

A. Metrics

The packet delivery ratio is the number of data packets received at the gateways divided by the number sent. The end-to-end delay is the mean delay of the received packets. The exposure is the share of gateway selections for which the route to the chosen gateway contained a node that was dropping at that moment; this uses the ground truth and is a measure, not an input of the policy. A switch is a change of the gateway of a flow. The detection rate and the false-positive rate are the shares of observer–dropping-node pairs, respectively of honest pairs, whose trust is below θ .

B. Handling of simulation runs

In some runs the simulator did not finish within a wall-clock limit of 110 s, which we attribute to the simulator and not to the protocol. Such a run was repeated with another seed (the original seed plus 1000, 2000 and so on). Of the 138 completed runs of the whole study, 55 had to be repeated in this way at least once, and for the 0 % setting one seed (4) could not be completed for either policy, so that these settings have nine runs. Because the repeated runs are spread over all settings, we do not expect a systematic effect on the comparison, but we state it for transparency.

V. RESULTS AND DISCUSSION

A. Delivery, delay, exposure and switching

Figure 3 shows the main results. With no dropping node the two policies gave practically the same delivery ratio, 0.981 ± 0.006 and 0.985 ± 0.005 . The delivery ratio of the nearest-gateway policy fell to 0.960 ± 0.013 , 0.937 ± 0.016 and 0.922 ± 0.021 for 10, 20 and 30 per cent of dropping nodes; for the trust-aware policy it was 0.965 ± 0.009 , 0.950 ± 0.014 and 0.936 ± 0.024 . The paired difference in delivery was 0.5, 1.3 and 1.5 percentage points; it was significant at the 5 % level only for 20 % ($p = 0.031$, better in 9 of 10 pairs), whereas for 10 % ($p = 0.39$) and 30 % ($p = 0.11$) it was positive but not significant with ten runs. The gain in delivery is therefore small and should be read as a tendency.

The effect on the exposure is clearer. The nearest-gateway policy selected a route with a dropping relay in 2.5, 3.9 and 5.9 per cent of the cases, the trust-aware policy in 1.3, 2.1 and 3.6 per cent. The paired reductions of 1.3, 1.8 and 2.3 percentage points were significant for all three shares ($p = 0.020$, 0.018 , 0.008). The absolute exposure is low because the gateways are close to most sources: the mean route length was about 1.2 hops, so most routes have no relay at all, and a dropping relay can only matter on the few routes that have one. In a larger network, or with the gateways at the edge, the exposure and the possible gain would be higher; this was not tested.

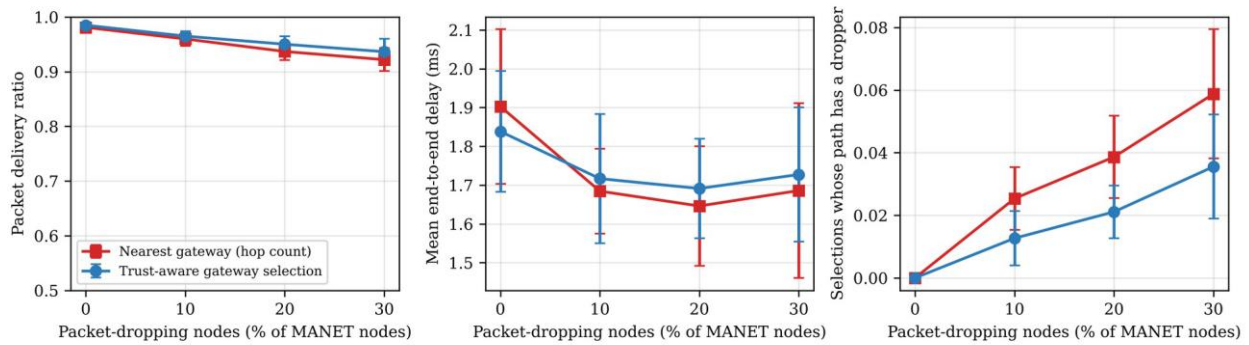


Figure 3. Packet delivery ratio (left), mean delay (centre) and exposure to dropping relays (right) for nearest-gateway (red) and trust-

aware (blue) selection.

The mean delay was between 1.7 and 1.9 ms for both policies, and the confidence intervals overlap; the trust-aware policy did not measurably increase the delay. The cost of the policy shows in the number of gateway switches per flow, which rose from 12.8 ± 2.9 to 19.7 ± 3.1 at 20 % of dropping nodes. The mean increase of about 7 switches was significant at every share ($p < 0.01$ at 10 %, 20 % and 30 %). A switch can interrupt a flow while the new route is set up, and a hysteresis rule that requires a minimum trust difference before switching is a natural remedy, which we did not evaluate.

Table 3. Delivery, exposure and switching, mean $\pm$ 95 % CI (paired difference trust minus nearest in the last column)

Dropping nodes	Policy	PDR	Exposure (%)	Switches / flow	Paired Δ PDR (pp)
0 %	nearest	0.981 ± 0.006	0.0 ± 0.0	15.0 ± 3.0	–
0 %	trust	0.985 ± 0.005	0.0 ± 0.0	15.8 ± 2.7	–
10 %	nearest	0.960 ± 0.013	2.5 ± 1.0	12.4 ± 2.4	–
10 %	trust	0.965 ± 0.009	1.3 ± 0.9	19.2 ± 2.1	$+0.5 \pm 1.1$
20 %	nearest	0.937 ± 0.016	3.9 ± 1.3	12.8 ± 2.9	–
20 %	trust	0.950 ± 0.014	2.1 ± 0.8	19.7 ± 3.1	$+1.3 \pm 1.0$
30 %	nearest	0.922 ± 0.021	5.9 ± 2.1	12.3 ± 1.9	–
30 %	trust	0.936 ± 0.024	3.6 ± 1.7	19.8 ± 4.2	$+1.5 \pm 1.6$

B. Route length and path trust of the selected routes

Table 4 shows what the two policies chose. The mean hop count of the selected route was almost the same for both policies (1.25 and 1.27 at 20 %), so the trust-aware policy did not pay for its safety with longer routes. The mean path trust of the selected routes was 0.926 ± 0.021 for the nearest-gateway policy and 0.947 ± 0.017 for the trust-aware policy at 30 % of dropping nodes; the policy thus moves the traffic to routes whose weakest relay has a higher trust, although the difference is small because most routes are direct or have a single relay. Exposure was not reduced to zero, which we have not traced to a single cause; candidates are the first slots of a flow, when few observations exist, and the 10 s between selections, during which routes change.

Table 4. Hop count and path trust of the selected routes, mean $\pm$ 95 % CI

Dropping nodes	Policy	Hops	Path trust
0 %	nearest	1.28 ± 0.06	0.968 ± 0.006
0 %	trust	1.28 ± 0.06	0.967 ± 0.008
10 %	nearest	1.27 ± 0.05	0.949 ± 0.013
10 %	trust	1.30 ± 0.04	0.959 ± 0.010
20 %	nearest	1.25 ± 0.04	0.940 ± 0.013
20 %	trust	1.27 ± 0.05	0.957 ± 0.010
30 %	nearest	1.27 ± 0.04	0.926 ± 0.021
30 %	trust	1.27 ± 0.05	0.947 ± 0.017

C. Accuracy of the trust values

Direct trust identified every dropping node that was observed: the detection rate was 100.0 ± 0.0 % at 10 % and 100.0 ± 0.0 % at 30 %, since a dropping node never forwards. The false-positive rate over honest pairs was 4.9 ± 1.9 %

with no dropping node and 2.4 ± 1.3 % with nine (Table 5). These accusations are most likely not the result of misbehaviour but of route breaks caused by mobility: a relay that has lost its next hop discards the packet that its neighbour has already counted as handed over. With truthful recommendations the network trust of honest nodes was about 0.84 and that of dropping nodes 0.09 to 0.14.

False recommendations changed the picture completely. With the mean aggregation the trust of honest nodes fell to 0.46 ± 0.03 at 10 % and 0.22 ± 0.02 at 30 %, so that 55.2 ± 9.6 % and 100.0 ± 0.0 % of the honest nodes were condemned and the detection rate of the real attackers dropped to 76.7 ± 13.9 % and 0.0 ± 0.0 %. The median was not much better (42.6 ± 10.8 % and 99.5 ± 0.9 % false positives), because each node is observed by only a few honest neighbours and the liars therefore outnumber the honest reports about almost every node. The trust-weighted mean reached 0.0 ± 0.0 % and 0.5 ± 0.9 % false positives and 100.0 ± 0.0 % and 90.0 ± 6.0 % detection, which is the accuracy of the truthful case, because the liars are themselves dropping nodes whose direct trust is low and whose reports therefore receive no weight.

Table 5. Detection (DR) and false-positive (FPR) rates in per cent, mean $\pm$ 95 % CI

Dropping nodes	Direct DR	Direct FPR	Mean (liars) FPR	Median (liars) FPR	Weighted (liars) DR	Weighted (liars) FPR
0 %	—	4.9 ± 1.9	3.3 ± 2.2	3.3 ± 1.5	—	3.0 ± 2.3
10 %	100.0 ± 0.0	1.6 ± 0.8	55.2 ± 9.6	42.6 ± 10.8	100.0 ± 0.0	0.0 ± 0.0
20 %	100.0 ± 0.0	2.1 ± 1.0	97.9 ± 1.4	89.2 ± 4.7	93.3 ± 5.3	0.0 ± 0.0
30 %	100.0 ± 0.0	2.4 ± 1.3	100.0 ± 0.0	99.5 ± 0.9	90.0 ± 6.0	0.5 ± 0.9

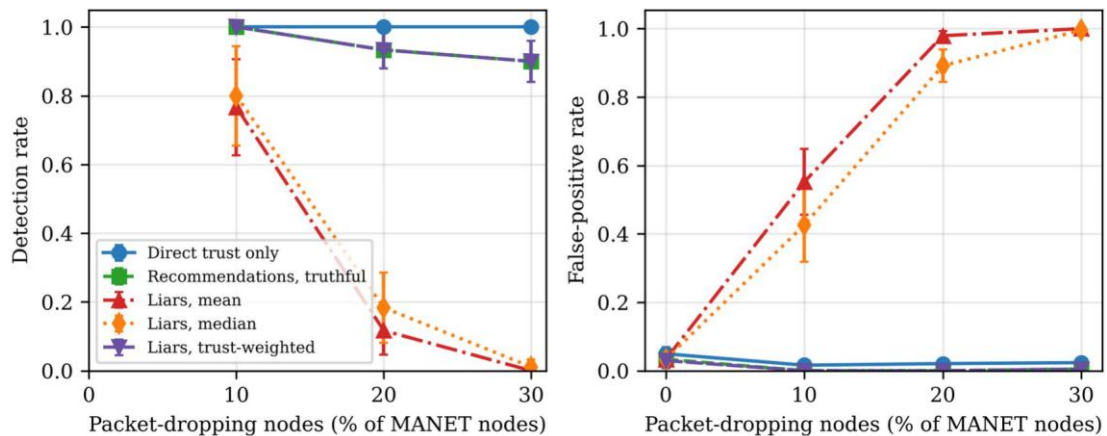


Figure 4. Detection rate (left) and false-positive rate (right) of direct trust and of the three aggregation rules, with and without lying

recommenders.

The two results connect. The online trust values that drove the gateway selection in Figure 3 were computed from truthful evidence. If the dropping nodes had also been allowed to lie, a mean or median aggregation would have marked honest relays as untrusted, and the selection would have avoided good routes and possibly pushed traffic towards the dropping nodes. The gain of the trust-aware selection thus depends on the defence in Algorithm 4.

D. Implications for trust-based adaptive gateway discovery

The experiment keeps the advertisement mechanism fixed and varies only the selection. The findings nevertheless indicate how trust and adaptation could be combined, and we state these points as design hypotheses that remain to be tested. First, an adaptive scheme that sets the advertisement range from the farthest active source [3] should count only the sources that can reach the gateway over trusted relays; otherwise the range is extended to cover nodes whose traffic would be lost on the way. Second, a node whose trust is below the threshold should not be allowed to forward advertisements, so that a dropping node cannot shape the proactive zone. Third, the advertisement interval could be shortened when the trust of the relays changes quickly, which is the case under on-off behaviour, and lengthened when it is stable. Finally, the gateway itself can contribute evidence, because it observes which sources stop delivering after a switch. These points connect the present results with the thesis topic of trust-based adaptive gateway discovery.

VI. LIMITATIONS AND THREATS TO VALIDITY

Internal validity is affected by the repeated seeds described in Section IV and by the idealised, truthful exchange of trust values. External validity is limited because the study used one simulator, one routing protocol, one radio model and a network in which the gateways are within a few hops of most nodes; results may differ for sparse networks, for reactive routing other than AODV and for a real radio channel with fading. Construct validity depends on the exposure measure, which uses the ground-truth state of the relays at the instant of the selection and does not follow the route afterwards, although routes change during the 10 s between selections.

The study uses one network size, one mobility setting, two gateways close to the centre, one threshold and one trust parameter set. The liars were also dropping nodes, which is why the trust-weighted mean works so well; a node that forwards correctly and lies only in its reports would keep its weight and would have to be countered by comparing its reports with the evidence of others. The online trust values assume a truthful exchange; the interaction of false recommendations with the selection was not simulated online. The watchdog false positives caused by route breaks were not corrected. Only the nearest-gateway and the trust-aware policies were compared; load-based and adaptive-zone policies were not included. The delivery gain is not significant for every share with ten runs, and a larger number of runs would be needed to narrow the confidence intervals.

VII. CONCLUSION

The paper evaluated a trust-aware selection of the gateway in an integrated Internet-MANET in which some nodes drop the packets they relay. Compared with the nearest gateway, it cut the exposure to dropping relays significantly for all shares of attackers and raised the delivery ratio by one to one and a half percentage points at 20 and 30 per cent attackers (significant at 5 % only for 20 %), at the price of more gateway switches. The trust values on which the selection relies were accurate when opinions were truthful; when the dropping nodes lied, mean and median aggregation failed, and only weighting opinions by the trust of their sender restored the accuracy. A trust-based gateway discovery should therefore combine a route-aware selection with a defence against false recommendations. Future work will add the adaptive advertisement range to the selection, evaluate the lying attack online, use hysteresis against unnecessary switching, and consider larger networks.

DECLARATIONS

AI-use statement. AI tools were used to assist with language editing, drafting support and preparation of figures. The research question, simulations, manuscript and conclusions are the authors' own, and all methods, results and technical content were verified by the authors, who take full responsibility for this work. **Conflict of interest.** The authors declare no conflict of interest. **Funding.** No external funding was received for this work. **Data availability.** The ns-3 scenario, the raw evidence files and the analysis scripts are available from the corresponding author on request.

REFERENCES

- [1] A. Hamidian, U. Körner, and A. Nilsson, "Performance of Internet access solutions in mobile ad hoc networks," in *Lecture Notes in Computer Science*, vol. 3427. Berlin, Germany: Springer, 2005, pp. 189–201.
- [2] R. U. Zaman, K. U. R. Khan, and A. V. Reddy, "A survey of adaptive gateway discovery mechanisms in heterogeneous networks," *Int. J. Computer Network and Information Security*, vol. 2013, no. 7, pp. 34–42, 2013.
- [3] P. M. Ruiz and A. F. Gomez-Skarmeta, "Maximal source coverage adaptive gateway discovery for hybrid ad hoc networks," in *Ad-Hoc, Mobile, and Wireless Networks (Lecture Notes in Computer Science*, vol. 3158). Berlin, Germany: Springer, 2004, pp. 28–41.
- [4] P. M. Ruiz and A. F. Gomez-Skarmeta, "Adaptive gateway discovery mechanisms to enhance Internet connectivity for mobile ad hoc networks," *Ad Hoc & Sensor Wireless Networks*, vol. 1, no. 1–2, pp. 159–177, 2005.
- [5] J.-H. Cho, A. Swami, and I.-R. Chen, "A survey on trust management for mobile ad hoc networks," *IEEE Commun. Surveys Tuts.*, vol. 13, no. 4, pp. 562–583, 2011.
- [6] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in *Proc. 6th Annu. Int. Conf. Mobile Computing and Networking (MobiCom)*, 2000.
- [7] A. Jøsang and R. Ismail, "The Beta reputation system," in *Proc. Bled Electronic Commerce Conf.*, Bled, Slovenia, June 2002.
- [8] Y. Sun, Z. Han, W. Yu, and K. J. R. Liu, "Attacks on trust evaluation in distributed networks," in *Proc. Conf. Information Sciences and Systems (CISS)*, 2006, pp. 1461–1466.
- [9] K. Hoffman, D. Zage, and C. Nita-Rotaru, "A survey of attack and defense techniques for reputation systems," *ACM Comput. Surv.*, vol. 42, no. 1, 2009.
- [10] R. U. Zaman, S. S. Begum, K. U. R. Khan, and A. V. Reddy, "Efficient adaptive path load balanced gateway management strategies for integrating MANET and the Internet," *Int. J. Wireless and Microwave Technologies*, no. 2, pp. 57–75, 2017.
- [11] R. U. Zaman, H. M. Alam, and K. U. R. Khan, "Improvement of adaptive load balanced gateway discovery protocol in hybrid integrated Internet-MANET," *Int. J. Interactive Mobile Technologies*, vol. 11, no. 3, 2017.
- [12] S. Buchegger and J.-Y. Le Boudec, "Performance analysis of the CONFIDANT protocol," in *Proc. ACM Int. Symp. Mobile Ad Hoc Networking and Computing (MobiHoc)*, 2002, pp. 226–236.

- [13] P. Michiardi and R. Molva, "CORE: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks," in *Advanced Communications and Multimedia Security*, IFIP vol. 100. Boston, MA: Springer, 2002, pp. 107–121.
- [14] A. Jøsang, R. Ismail, and C. Boyd, "A survey of trust and reputation systems for online service provision," *Decision Support Systems*, vol. 43, no. 2, pp. 618–644, 2007.
- [15] Y. L. Sun, W. Yu, Z. Han, and K. J. R. Liu, "Information theoretic framework of trust modeling and evaluation for ad hoc networks," *IEEE J. Sel. Areas Commun.*, vol. 24, no. 2, pp. 305–315, 2006.
- [16] I.-R. Chen, J. Guo, F. Bao, and J.-H. Cho, "Trust management in mobile ad hoc networks for bias minimization and application performance maximization," *Ad Hoc Networks*, vol. 19, pp. 59–74, 2014.
- [17] R. U. Zaman and R. Sultana, "Identifying trustworthy nodes in an integrated Internet MANET to establish a secure communication," in *Advances in Intelligent Systems and Computing*, vol. 712. Singapore: Springer, 2018, p. 321 ff.
- [18] R. U. Zaman, A. V. Reddy, M. A. Raheem, and K. U. R. Khan, "Contemporary trust management strategies for establishing secure communication in the heterogeneous network," *Int. J. Sci. Res. Rev.*, vol. 8, no. 2, pp. 2075–2093, 2019.
- [19] C. Perkins, E. Belding-Royer, and S. Das, "Ad hoc On-Demand Distance Vector (AODV) routing," RFC 3561, IETF, July 2003.
- [20] G. F. Riley and T. R. Henderson, "The ns-3 network simulator," in *Modeling and Tools for Network Simulation*. Berlin, Germany: Springer, 2010, pp. 15–34.