



# **iJRASET**

International Journal For Research in  
Applied Science and Engineering Technology



---

# **INTERNATIONAL JOURNAL FOR RESEARCH**

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

---

**Volume:** 14      **Issue:** X      **Month of publication:** October 2026

**DOI:** <https://doi.org/10.22214/ijraset.2026.85180>

**[www.ijraset.com](http://www.ijraset.com)**

**Call:** ☎ 08813907089

**E-mail ID:** [ijraset@gmail.com](mailto:ijraset@gmail.com)

# Trust-Based Adaptive Gateway Discovery in Integrated Internet-MANET: A Review of Mechanisms, Trust Models and Open Issues

Mohammed Abdul Raheem<sup>1</sup>, Khaleel Ur Rahman Khan<sup>2</sup>

<sup>1</sup>Research Scholar, Rayalaseema University, Kurnool, India

<sup>2</sup>ACE Engineering College, Hyderabad, India

**Abstract:** *An integrated Internet-MANET lets mobile nodes reach the Internet through gateways, and the mechanism by which a node finds and chooses a gateway has a large effect on delivery, delay and overhead. Adaptive versions of this mechanism adjust the advertisement range and interval to the network, but they treat every node as cooperative, which is not true in an open network where nodes drop packets or send false information. This paper reviews gateway discovery and its adaptive variants, the attacks that threaten them, and the trust models that can be used against these attacks. It then organises the design space of trust-based adaptive gateway discovery into four dimensions: the discovery mechanism, the selection metric, the trust evidence and the attack resilience. Algorithms for trust-aware gateway selection and for trust-weighted aggregation of recommendations are given as a reference design, and the open issues are collected: newcomers, on-off behaviour, false recommendations, the overhead of evidence, the integration of trust with the adaptation of the advertisement range, and the lack of common benchmarks. The review is intended as a starting point for researchers who work on secure Internet connectivity for mobile ad hoc networks.*

**Keywords:** *Integrated Internet-MANET, gateway discovery, adaptive gateway discovery, trust management, reputation, security, review*

## I. INTRODUCTION

A mobile ad hoc network (MANET) is formed by mobile devices that relay each other's packets without any fixed infrastructure. Its range is limited, and many applications need access to the Internet as well. The two networks complement each other: the Internet offers global reach and services, and the MANET offers connectivity where no infrastructure exists. They are joined by gateways, nodes that have an interface to the wired network and an interface to the ad hoc network [1, 2].

To use a gateway a mobile node has to discover it, register with it, and send its packets over the multi-hop route to it. Discovery can be proactive, with periodic advertisements by the gateway, reactive, with solicitations by the node, or hybrid. The size of the proactive zone and the advertisement interval decide the balance between overhead and delay, and a large body of work has proposed to adapt them to the network [2, 3, 4]. Once more than one gateway is available, the node must also choose among them, and the criteria used for this choice have included the number of hops, the load and the stability of the path [5, 6].

Nearly all of this work takes the cooperation of the nodes for granted. In practice nodes can be selfish, faulty or compromised. A node on the route to a gateway can accept packets and drop them, a node can send false advertisements or false opinions, and a node can behave well and badly in turn to escape detection.

Trust management addresses such behaviour in ad hoc networks by letting nodes judge each other from evidence [7]. Combining the two areas gives the topic of this review, trust-based adaptive gateway discovery, which is also the subject of the first author's doctoral research.

The contributions of the review are: (1) a compact account of gateway discovery and of the adaptive schemes in a common vocabulary; (2) a catalogue of the attacks that affect gateway discovery, with the trust mechanisms that address them; (3) a taxonomy and a reference design, with algorithms, for trust-based adaptive gateway discovery; and (4) a list of open issues with the reasons why they matter. The remainder of the paper is organised along these lines.

## II. INTEGRATED INTERNET-MANET AND GATEWAY DISCOVERY

### A. Architecture

Figure 1 shows the architecture. Mobile nodes form a multi-hop network, and one or more gateways connect to the Internet. A source that wants to reach a host in the Internet sends its packets to a gateway, which forwards them, and the reverse path is followed for the replies. Mobile IP functions can be added so that a node keeps its address when it moves between the zones of different gateways [1]. The links among the nodes are wireless, so a route to a gateway can break when a node moves, and the routing protocol, in this paper AODV [8], must repair it.

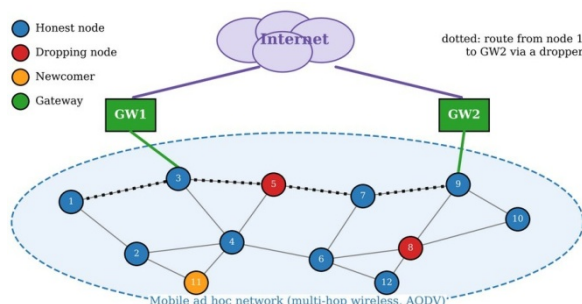


Figure 1. Architecture of an integrated Internet-MANET with two gateways. A trust-aware source avoids the route through the dropping node

### B. Proactive, reactive and hybrid discovery

In proactive discovery the gateway broadcasts an advertisement message at regular intervals. A time-to-live field limits how many hops the message travels, so the gateway advertises only within a zone. A node that hears an advertisement can register at once, so the delay of discovery is short, but the advertisements load the network even when no node needs the gateway. In reactive discovery the node broadcasts a solicitation when it needs a gateway and the gateway answers. No overhead is spent when nothing is needed, but the first packet waits for the discovery. In hybrid discovery the nodes inside the proactive zone use advertisements, and the nodes beyond it use solicitations (Figure 2). The hybrid approach is the most flexible, and it raises the question of how the zone and the interval should be set [1, 2]. Table 1 summarises the three approaches.

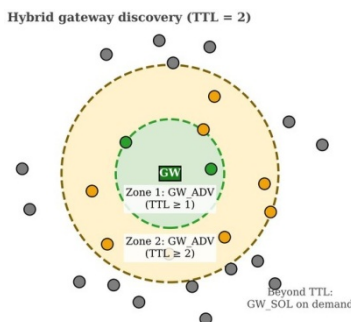


Figure 2. Hybrid gateway discovery with a time-to-live of two hops. Green and amber nodes receive advertisements; grey nodes solicit.

Table 1. Gateway discovery approaches

| Approach  | Trigger                                     | Overhead        | Delay         |
|-----------|---------------------------------------------|-----------------|---------------|
| Proactive | Periodic advertisement                      | High, constant  | Short         |
| Reactive  | Solicitation by node                        | On demand       | Longer        |
| Hybrid    | Advertisement in zone, solicitation outside | Depends on zone | Short in zone |

### C. Registration, handover and gateway choice

Discovery is followed by registration. In an integrated network that uses Mobile IP, the node obtains a care-of address from the gateway whose advertisement it has heard, registers it with its home agent, and from then on its packets and the replies pass through that gateway. A node that moves out of the zone of its gateway must register again, and the time this takes appears as a break in the flow. When a node hears more than one gateway, the choice among them is a policy decision that the discovery mechanism does not settle. The usual policies are the nearest gateway, the least loaded gateway, and combinations of hop count with the load or stability of the path [1, 5]. Each has a typical failure: the nearest gateway can be overloaded, and the least loaded gateway can be far away. A policy based on trust adds a third criterion that addresses a different failure, the loss of packets on a route that is short and lightly loaded but passes a node that does not forward.

The cost of a wrong choice also depends on the application. A bulk transfer can survive a few lost packets and a delayed registration, whereas an interactive session cannot, and a source that has chosen a gateway through a dropping node may notice only through the retransmission timers of the transport layer, which react slowly. A mechanism that detects misbehaviour early in the network layer, and moves the flow before the transport layer has timed out, gives the largest benefit for applications of the second kind.

## III. ADAPTIVE GATEWAY DISCOVERY

A static zone and a static interval fit one network condition only. When the nodes are dense, a large zone floods the network with advertisements that few nodes need; when they are sparse, a small zone leaves nodes without a gateway. Adaptive schemes therefore change the advertisement range, the advertisement interval, or both, while the network runs. They can be classed as adapting the range only, the interval only, or both [2].

Ruiz and Gomez-Skarmeta proposed to set the range from the active sources: the maximal source coverage scheme extends the advertisements as far as the most distant node that is sending data through the gateway, and they also considered the average and the minimal source distances [3, 4]. A benefit-oriented variant compares the cost of flooding the network with advertisements against the cost of serving sources without them, and chooses the range that gives the largest benefit [2, 4]. Other proposals reviewed in [2] adapt the range by checking the distribution of registered nodes at intervals, use the degree of movement of nodes, apply fuzzy control, or use an evolutionary algorithm to tune the interval; one distributed scheme lets the nodes themselves take part in deciding how far advertisements travel. Load-balanced management of the gateways, which spreads the sources over the gateways according to the load of the gateways and of the paths to them, is treated in [5, 6].

Table 2. Adaptive discovery: what is adapted

| Class | Adapted quantity          | Examples               |
|-------|---------------------------|------------------------|
| A     | Advertisement range (TTL) | Source coverage [3, 4] |
| B     | Advertisement interval    | Tuned interval [2]     |
| C     | Range and interval        | Combined schemes [2]   |

The adaptation metrics in these schemes are traffic, distance, mobility and load. None of them depends on whether the nodes that carry the traffic can be trusted. If an adaptive scheme extends the zone to cover a source whose route passes a dropping node, it increases the overhead and does not improve delivery.

Several limits are common to the adaptive schemes. First, they react to the sources that are active now, so a short burst of traffic can change the range and then change it back, and the advertisement sent in between are wasted. Second, the range and the interval are set by the gateway on its own, from information that it collects from the data packets that pass it; this is cheap, but the gateway sees only the sources that already use it. Third, the schemes were evaluated mostly in simulations with cooperative nodes, so their behaviour under misbehaviour is not known. Fourth, when several gateways serve one network, the adaptation of each gateway is independent of the others, and the zones can overlap or leave gaps. A trust-aware scheme has to handle the same limits and, in addition, the uncertainty of the trust values, which is why the adaptation should not react to every small change of trust.

We summarise the strengths and weaknesses in Table 3. The comparison is qualitative, since the schemes were evaluated in different simulators and scenarios, which is itself one of the open issues listed in Section VII.

Table3.Strengthsandlimitsoftheadaptiveapproaches

| Adaptedquantity     | Strength               | Limit              |
|---------------------|------------------------|--------------------|
| Range only          | Itsneedlessflooding    | Fixed interval     |
| Intervalonly        | chestrafficandmobility | Fixed zone         |
| Rangeand interval   | Mostflexible           | estate,more tuning |
| Distributeddecision | Usesnodeinformation    | More messages      |

#### IV. SECURITY THREATS TO GATEWAY DISCOVERY

Table 4 lists the threats that matter for gateway discovery. The first group acts on the data path. A blackhole node attracts traffic by taking part in route discovery and then drops everything; a grayhole drops selectively or part of the time. On-off nodes alternate good and bad periods so that they are judged by their good behaviour [9]. The second group acts on the discovery itself. A node could forge or replay advertisements to attract registrations, or refuse to forward the advertisements of a gateway, so that nodes beyond it are not reached by the proactive zone. The third group acts on the trust evaluation. Bad-mouthing and ballot stuffing distort recommendations, a Sybil attacker multiplies its identities, and whitewashing lets a node discard a bad record by rejoining under a new identity [9, 10].

Table4.Threatsandtheireffectongatewaydiscovery

| Threat                   | Effectongateway discovery         |
|--------------------------|-----------------------------------|
| Blackhole, grayhole      | hthechosengatewayislost           |
| On-offbehaviour          | ustedingoodphases,andevidenceages |
| Forged advertisement     | steratafalseordistantgateway      |
| Advertisementsuppression | Proactivezoneshrinks;delaygrows   |
| Bad-mouthing,stuffing    | scondemned,badrelayspraised       |
| Whitewashing, Sybil      | ased;newcomersover-trusted        |

The effect of the first group is easy to see: agateway that is nearest in hops is not the best choice if the route to it contains a dropping node. The effect of the second group is also direct but depends on the discovery mechanism, and authentication of advertisements is the usual remedy. The third group is the most subtle, because a defence that relies on trust inherits all the weaknesses of the trust evaluation. This is why a review of trust-based gateway discovery must look at the trust models themselves.

Defences exist for every threat in Table 4, but they sit in different layers. Authentication of advertisements by the gateway, for example with a signature or a sharedkey,preventsforgedadvertisements,butitneeds key management in a network without fixed infrastructure, which is hard. Multipath and redundant gateways reduce the damage of a dropping nodewithout identifying it, at the price of overhead. Detection by monitoring and reputation identifies the node and lets it be excluded, and it is the approach considered in this review because it needs no keys and works with the routing protocol as it is. These approaches are complementary: authentication limits who may advertise, trust limits who may relay, and redundancy limits the cost of the relays that have notyet been identified. A furtherpointistheinteractionbetweenthethreats and the adaptation of the discovery. A proactive zone that shrinks because advertisements are suppressed looks, to an adaptive scheme that measures coverage, like a change in the node population, and the scheme may respond by raising the range, which sends more advertisements into the area where they are being suppressed. A trust-aware scheme can use the trust of the forwarders to tell the two causes apart.

## V. TRUST MODELS FOR ADHOC NETWORKS

### A. Evidence

The watchdog of Marti et al. [11] is the best-known source of direct evidence. Another that hands a packet to a neighbour listens to see whether the neighbour passes it on, and counts the outcomes. The mechanism needs promiscuous reception, and it is affected by collisions, by limited power and by routes that break; a relay that has lost its next hop drops a packet without any intent to do so, so a watchdog produces some false accusations in a mobile network. Acknowledgements from the destination are an alternative that avoids overhearing but gives evidence about a whole path, not about single nodes.

### B. Reputation and trust computation

CONFIDANT combines monitoring, a reputation system, a trust manager and a path manager, and distributes warnings about misbehaving nodes [12]. CORE keeps subjective, indirect and functional reputation and lets only positive indirect information raise a reputation, so that a false negative opinion cannot be used to slander a node [13]. The Beta reputation system represents the evidence of positive and negative outcomes by a Beta distribution, whose expected value is the trust [14]. Sun et al. derive trust from entropy and from probability, and show how to propagate it through a chain of nodes [15]. Surveys of the area are given in [7, 16, 17]. Table 5 compares the models by the features that matter for a gateway selection.

Table 5. Trust models and their use

| Model                      | Evidence             | Notable feature        |
|----------------------------|----------------------|------------------------|
| Watchdog/pathrater [11]    | Overheard forwarding | Direct, simple         |
| CONFIDANT [12]             | Observation, reports | Warnings, path manager |
| CORE [13]                  | Observation, reports | Positive-only indirect |
| Beta [14]                  | Counts of outcomes   | Expected value, prior  |
| Information-theoretic [15] | Observation, reports | Propagation of trust   |

Several design choices recur across these models and matter for gateway selection. The first is the granularity of the evidence: per packet, per flow or per time slot. Slots make the computation light and make the effect of forgetting easy to state. The second is the minimum amount of evidence needed before a node is classified; below it the trust remains at the initial value. The third is whether trust is local to each node or shared as a network-level value; a shared value reacts faster but is exposed to false reports. The fourth is the treatment of the trust of the path, which can be the product of the trust of the relays, as in a probability of successful forwarding, or their minimum, as in a weakest-link rule. The product reflects the chance of delivery along the route, and the minimum reflects the idea that a single bad relay is enough to disqualify the route; the minimum is also less sensitive to the number of relays and therefore does not penalise long routes through trusted nodes.

### C. Parameters of the Beta model

In the Beta model the trust of node  $j$  seen by node  $i$  is  $T = (r + w \cdot T_0) / (r + s + w)$ , where  $r$  and  $s$  are the counts of good and bad outcomes,  $T_0$  is the initial trust and  $w$  the weight of the prior (Algorithm 1). Two further parameters appear in practice. A forgetting factor discounts old evidence, and a decision threshold  $\theta$  separates trusted from untrusted nodes. The initial trust matters for a node that has just joined, since it fixes whether the node is trusted before any evidence exists; a value above the threshold invites whitewashing, and a value below it keeps honest newcomers out of the routes. The forgetting factor decides how fast an on-off node can recover its standing. These parameters interact with the decision rule in ways that are not obvious, and we regard their evaluation in a gateway setting as a main open issue.

#### Algorithm1. Betatrustwithforgettingandinitial trust

1. Input: counters  $r(i,j)$ ,  $s(i,j)$ ; prior weight  $w$ ; initial trust  $T_0$ ; forgetting factor  $\lambda$ ; 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. Recommendations

Direct evidence is sparse in a mobile network, since a node sees a given neighbour for a short time only. Nodes therefore exchange their trust values, and the aggregate of the reports is used. A simple mean is easily moved by liars, and a median helps only while the liars are fewer than half of the reporters for each node. A common remedy is to weight each report by the trust of its sender, so that reports from nodes with low trust count little (Algorithm 2). This works against liars that are also misbehaving on the data path, but it does not help against a node that forwards correctly and lies about others; for that case the reports must be checked against independent evidence. Recommenders that are themselves newcomers pose a further problem, since their trust is the initial value.

#### Algorithm2. 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

## VI. TRUST-BASED ADAPTIVE GATEWAY DISCOVERY

#### A. Designspace

Figure 3 organises the design space along four dimensions. The discovery mechanism is proactive, reactive or hybrid, with or without adaptation. The selection metric is the hop count, the load of the gateway or of the path, or the trust of the path. The trust evidence is direct, recommended or a combination. The attack resilience describes which of the threats of Table 4 the scheme withstands. A concrete scheme is a point in this space, and a trust-based adaptive scheme is one in which the trust enters the selection metric or the adaptation, or both.

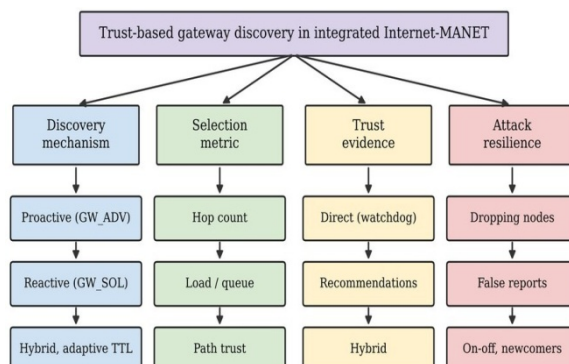


Figure3. Taxonomy of trust-based gateway discovery along four dimensions.

### B. Where trust can enter

Trust can enter the scheme at five points. (1) Selection: a source chooses among the gateways by the path trust instead of, or together with, the hop count.

(2) Advertisement forwarding: a node whose trust is low is not allowed to forward advertisements, so that it cannot shape the proactive zone. (3) Range adaptation: the maximal source coverage is computed over the sources whose routes pass only trusted relays. (4) Interval adaptation: the interval is shortened when the trust of the nodes in the zone changes quickly, because the information about the nodes then ages fast. (5) Registration and load balancing: a gateway weights the registrations it accepts and the load it assigns by the trust of the source and of its path. Table 6 lists these points with the data they need.

Table 6. Points at which trust can enter the scheme

| Point                        | Trust input              | Output                |
|------------------------------|--------------------------|-----------------------|
| Gateway selection            | Path trust               | Chosen gateway        |
| Advertisement forwarding     | Trust of forwarder       | Allow/block           |
| Range (TTL) adaptation       | Trust of sources' routes | TTL value             |
| Interval adaptation          | Rate of trust change     | Interval              |
| Registration, load balancing | Trust of source, path    | Admission, load share |

### C. Referenced design for the selection

The first point is the best understood. The source reads the route to each gateway and computes the path trust as the smallest trust among the relays, so that a single untrusted relay makes the route untrusted. Among the routes that pass the threshold it takes the shortest, and if none passes it takes the route with the highest path trust (Algorithm 3 and Figure 4). The rule keeps the hop-count preference of the conventional scheme where the network is healthy and changes the choice only when a route contains a relay that is not trusted. A hysteresis rule should be added in a practical scheme so that the source does not oscillate between gateways when the trust values are close to the threshold. The first author's simulation studies of this design in ns-3 are being prepared for publication and are not discussed here.

Algorithm 3. Trust-aware gateway selection by a source node

1. Input: gateways  $G$ , sources, threshold  $\theta$ , period  $10s$
2. Every  $10s$ , 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.  $hops(g) = \text{number of hops}$ ;  $R(g) = \text{relay nodes on the route}$
  5.  $PT(g) = \min \{ T(r) \mid r \in R(g) \}$  ( $PT(g) = 1$  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  $g$

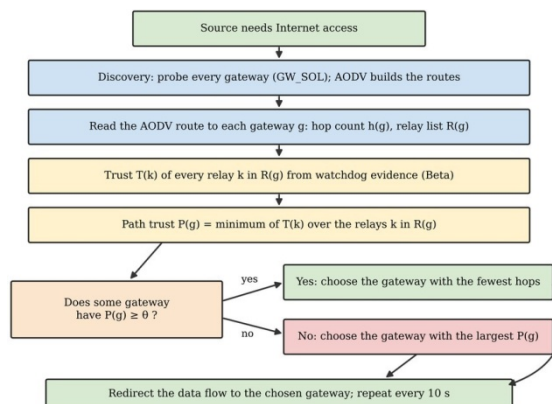


Figure4.Flowofthetrust-awaregatewayselection

The related published work of the group has examined trusted gateway selection and trust management for integrated networks [18, 19], the adaptive discovery of gateways [2] and load-balanced gateway management [5, 6]. The reference design joins these themes. In an implementation the source does not normally know the whole route, so the path trust must come from a route record, from a field carried in the route reply, or from reports of the nodes on the route.

#### D. A worked example of the selection

Take a source with two gateways and a threshold of

0.5. The route to gateway 1 has two hops and one relay with network trust 0.28; the route to gateway 2 has three hops and two relays with trust 0.84 and 0.77. The path trust of the first route is 0.28 and that of the second is 0.77, so only the second passes the threshold and is chosen, although it is longer; a conventional scheme would take the first. If the trust of the first relay later rises above 0.5, for example because it has forwarded correctly for a while, the first route passes as well and the source returns to it, as it has fewer hops. If both routes were below the threshold, the source would take the one with the higher path trust. Table 7 gives the outcome of each policy.

Table7.Example of the choice

| Route    | Hops | Path trust | Nearest | Trust-aware |
|----------|------|------------|---------|-------------|
| Gateway1 | 2    | 0.28       | chosen  | rejected    |
| Gateway2 | 3    | 0.77       | –       | chosen      |

#### E. Trust-aware range adaptation

The third point of Section VI-B extends the maximal source coverage scheme. The gateway keeps the hop distance of each active source and, in addition, a flag that tells whether the route of the source passes only trusted relays. The new range is the largest distance among the sources that carry the flag, so that a source behind a doubtful relay does not push the range outwards. The scheme is a design proposal and has not been evaluated; Algorithm 4 states it.

Algorithm4.Trust-aware range(TTL) adaptation at a gateway

1. Input: active sources  $S$ , hop distance  $h(s)$ , router relays  $R(s)$ , threshold  $\theta$ , bounds  $TTL_{min}$ ,  $TTL_{max}$
2. For each active source  $s$  in  $S$ :
  3.  $PT(s) = \min$  of  $T(r)$  over  $r$  in  $R(s)$
  4. if  $PT(s) \geq \theta$  then add  $s$  to the trusted set  $S_T$
5. If  $S_T$  is empty then  $TTL = TTL_{min}$
6. Else  $TTL = \max$  of  $h(s)$  over  $s$  in  $S_T$
7.  $TTL = \min(TTL_{max}, \max(TTL_{min}, TTL))$
8. Send the next GW\_ADV with this TTL; forward it only through nodes with  $T \geq \theta$
9. Recompute at every advertisement interval

The rule has two effects. It saves advertisements that would otherwise be spent on sources that cannot reach the gateway reliably, and it denies untrusted nodes the role of an advertisement forwarder. It also has a risk: a source that is excluded from the zone must still be able to find a gateway by solicitation, and the reactive path must therefore remain open. If the trust values are wrong, the range can be set too small, which is a lower bound and a slow change of the range limit.

#### F. Implementation considerations

Several practical points decide whether the reference design can be deployed. The evidence collection needs a node to overhear its neighbours, which is available in most wireless interfaces but costs energy, so a node may sample the transmissions instead of observing all of them. The state per node grows with the number of neighbours that it observes, which is small in a MANET of moderate size. The path trust can be carried in the route reply as one field, filled by every relay with the minimum of its own trust value and the value already in the field, which gives the source the weakest-link value at no extra message; the field must be protected against tampering, since a relay can otherwise raise it. The probes that keep a route to every gateway alive are small, and their period trades overhead against the freshness of the route. Finally, the re-selection period should be longer than the time a route needs to be repaired, otherwise the source reacts to the transient state of the routing protocol and not to the trust.

#### G. Complexity

The cost of the selection at a source is linear in the number of gateways and in the length of the routes, and the cost of the trust update at an observer is linear in the number of neighbours that it observes. The exchange of reports is the expensive part, since in the worst case each node reports about every other node; limiting the reports to the neighbours and to the nodes on the routes in use reduces the cost to the number of observed pairs. These costs are small beside the cost of the data traffic in the scenarios that are usually simulated, but they should be measured and reported.

## VII. EVALUATION PRACTICE AND OPEN ISSUES

### A. Evaluation

A fair evaluation of a trust-based gateway scheme needs metrics from three areas. Network metrics are the packet delivery ratio, the end-to-end delay, the control overhead and the number of gateway switches. Security metrics are the detection rate, the false-positive rate, the delay of detection and the exposure, defined as the share of selections whose route contains a node that is misbehaving at that time. Trust metrics are the accuracy of the trust values and the time to recover after a change of behaviour. The simulator should state the radio model, the mobility, the placement of the gateways and the number of runs, and report confidence intervals; ns-3 [20] and its AODV implementation are suitable for this. Many published studies use a single run per point and a single attacker density, which does not support conclusions about small differences.

The main metrics can be stated precisely. With  $N_{\text{sent}}$  data packets sent and  $N_{\text{recv}}$  received, the delivery ratio is  $\text{PDR} = N_{\text{recv}} / N_{\text{sent}}$ . The exposure of a policy over  $K$  selections, of which  $K_{\text{bad}}$  were made when the chosen route contained a node that was dropping, is  $E = K_{\text{bad}} / K$ . The detection rate is  $\text{DR} = \text{TP} / (\text{TP} + \text{FN})$  and the false-positive rate is  $\text{FPR} = \text{FP} / (\text{FP} + \text{TN})$ , computed over nodes or over observer-node pairs, and the control overhead is the number of control bytes divided by the number of data bytes delivered.

$$\text{PDR} = N_{\text{recv}} / N_{\text{sent}}, E = K_{\text{bad}} / K, \text{DR} = \text{TP} / (\text{TP} + \text{FN}), \text{FPR} = \text{FP} / (\text{FP} + \text{TN}) \quad (2)$$

Three factors of the scenario deserve attention because they change the conclusions. The first is the placement of the gateways. If the gateways lie at the centre of the area, most sources are one or two hops away, there are few relays to be trusted or distrusted, and the benefit of a trust-aware choice is small; if the gateways lie at the edge, routes are long, and the choice between gateways is a choice between whole sets of relays. The second is the density of the network: in a dense network several routes to each gateway exist, and the routing protocol itself can avoid a bad relay if the evidence is given to it, which suggests that trust should also be fed into the route discovery, not only into the choice of the gateway. The third is mobility. A high mobility makes the evidence short-lived, raises the false accusations of the watchdog, and makes the forgetting factor more important; a low mobility makes a one-time classification of a node sufficient.

### B. Open issues

- **Newcomers.** The value given to a node without history is a design choice with a cost on both sides: honest newcomers wait, or malicious ones are trusted. Sources of initial evidence other than the watchdog, for example the registration at the gateway, are largely unexplored.

- On-off and forgetting. The choice of the forgetting factor balances the memory of past misbehaviour and the readmission of nodes that have repaired. An asymmetric rule, in which bad evidence is forgotten more slowly than good evidence, is a candidate that needs study.
- False recommendations. Weighting by the trust of the sender handles liars that also drop packets. Liars that forward correctly, collusion and Sybil identities need further mechanisms.
- Evidence quality. Route breaks produce false accusations by a watchdog. A model that separates mobility losses from misbehaviour would improve every trust scheme.
- Overhead and energy. Promiscuous reception, the exchange of reports and the extra probes cost energy and bandwidth. The trade-off between the accuracy of trust and the overhead of evidence has not been mapped.
- Joint adaptation. The adaptation of the advertisement range and interval and the adaptation of the trust parameters should be designed together; for example, a high trust turnover argues for shorter intervals.
- Benchmarks. There is no common scenario, attacker set or metric list for trust-based gateway discovery, so that results from different papers cannot be compared. A shared benchmark in ns-3 would be a useful contribution.

### C. Applications scenarios

Three kinds of deployment illustrate where the combination is useful. In an emergency response network, the nodes are carried by teams of different organisations that do not know each other, so the nodes cannot be assumed to cooperate, and the Internet access through a satellite or cellular gateway is critical. In a campus or community network, the nodes are owned by individuals, some of whom would prefer not to spend their battery on the packets of others, so selfish behaviour is the main threat. In a vehicular network that is connected to roadside units, the topology changes fast, newcomers arrive all the time, and the treatment of newcomers dominates the design. The reference design of this review can be adapted to all three, but the parameters, such as the threshold, the forgetting factor and the initial trust, need to be chosen for the setting.

### D. Relation to earlier surveys

Earlier surveys cover parts of this area. The survey of adaptive gateway discovery [2] reviews the mechanisms of Section III and does not consider security. The review of trust management for heterogeneous networks [19] and the survey of trust in MANETs [7, 16, 17] treat trust models in general and do not address gateway discovery. The present review is an attempt to connect the two bodies of work, and its main addition is the design space of Section VI together with the reference algorithms.

### E. Research roadmap

We suggest the following order of work. First, establish the benefit of trust-aware selection against nearest-gateway selection under packet-dropping nodes, with paired runs and confidence intervals, in networks of different density and different gateway placement. Second, study the parameters of the trust model, namely the initial trust, the prior weight, the forgetting factor and the threshold, in the same scenarios. Third, add the defence against false recommendations and test it against liars that also forward correctly. Fourth, combine the trust with the adaptation of the advertisement range and interval, and measure the overhead saved. Fifth, move from simulation to a testbed, where the false accusations by the watchdog under a real radio channel can be measured. Each step produces results that are useful by themselves, and together they would give a complete account of trust-based adaptive gateway discovery.

## VIII. CONCLUSION

Gateway discovery in an integrated Internet-MANET has been refined for years with respect to overhead and delay, but it still assumes cooperative nodes. This review put gateway discovery, its adaptive variants, the threats and the trust models in one frame. The design space has four dimensions, trust can enter a scheme at five points, and a reference algorithm for the selection of a gateway from path trust was given.

The main open issues are the treatment of newcomers, on-off behaviour and false recommendations, the cost of evidence, and the joint adaptation of the advertisement parameters and of the trust parameters. We expect the combination of adaptive gateway discovery and trust management to remain an active topic as networks of mobile devices grow.

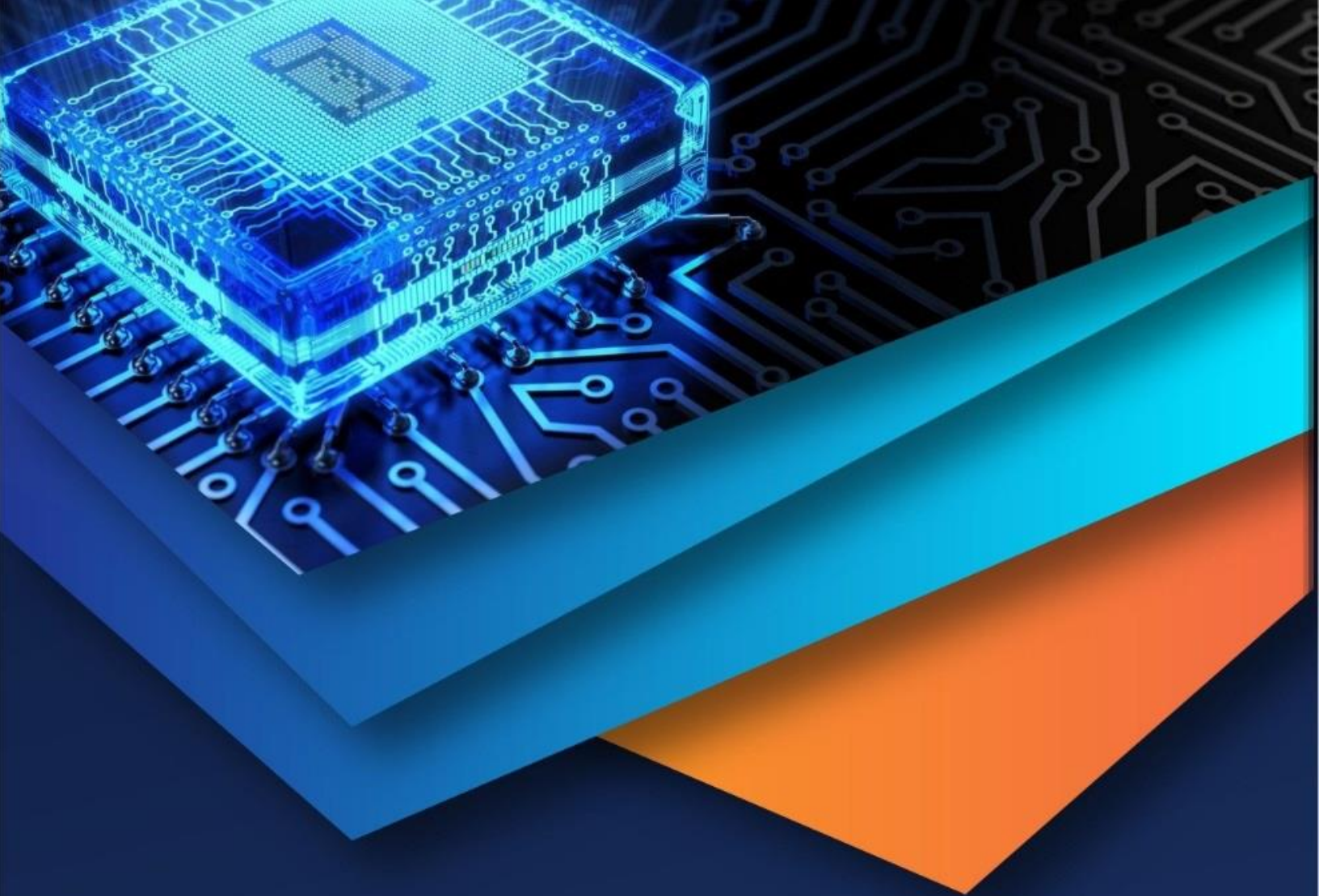
## IX. DECLARATIONS

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. Data availability. No new data were generated for this review.

## 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] 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.
- [6] 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.
- [7] 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.
- [8] C. Perkins, E. Belding-Royer, and S. Das, "Ad hoc On-Demand Distance Vector (AODV) routing," RFC 3561, IETF, July 2003.
- [9] 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.
- [10] 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.
- [11] 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.
- [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 and R. Ismail, "The Beta reputation system," in *Proc. Bled Electronic Commerce Conf.*, Bled, Slovenia, June 2002.
- [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] 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.
- [17] 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.
- [18] 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.
- [19] 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.
- [20] G. F. Riley and T. R. Henderson, "Thens-3 network simulator," in *Modeling and Tools for Network Simulation*. Berlin, Germany: Springer, 2010, pp. 15–34.



10.22214/IJRASET



45.98



IMPACT FACTOR:  
7.129



IMPACT FACTOR:  
7.429



# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089  (24\*7 Support on Whatsapp)