



A Trust-Aware Round-Trip-Time and Hop-Count Anomaly Approach for Wormhole Attack Detection in Mobile Ad Hoc Networks

¹ Ibrahim Salim M

¹ Assistant Professor, Department of Computer Applications,
MES College Marampally Ernakulam, India.

ABSTRACT- Mobile Ad hoc Networks (MANETs) route data cooperatively across nodes without any fixed infrastructure, which makes them flexible but also exposes them to attacks that exploit the routing layer directly. The wormhole attack is among the most disruptive of these: two colluding malicious nodes capture control or data packets at one point in the network, tunnel them through an out-of-band or high-speed link, and replay them at a distant point, creating the illusion of a short, attractive route that does not correspond to any real physical path. Because the tunnel can be established without breaking any cryptographic protection and without compromising any legitimate node, wormhole attacks are difficult to detect using authentication alone. This paper proposes a detection approach that combines two independent, lightweight signals — round-trip time (RTT) anomalies observed during route discovery and hop-count deviation relative to a locally estimated node density — with a slowly-decaying per-neighbor trust score, so that a single suspicious observation does not immediately convict a node, but a consistent pattern across multiple route discoveries does. The approach is presented at the design level, with its detection logic, thresholds, and expected trade-offs described in detail; no simulation results are reported here, and the discussion of evaluation is limited to the metrics and experimental design that would be needed to validate it.

Keywords: [MANET, Wormhole Attack, AODV, Round-Trip Time, Hop-Count Analysis, Trust Management, Intrusion Detection.]

1. INTRODUCTION

A Mobile Ad hoc Network (MANET) is formed on the fly by mobile devices that agree to relay each other's traffic, with no base station, router, or central administrator coordinating the network. This cooperative, infrastructure-free model is what makes

MANETs useful in settings like disaster response, military field operations, and temporary sensor deployments, but it is also the model's biggest security liability: every participating node is a potential point of failure or compromise, and the routing protocol itself has to be trusted at face value by default.

Reactive routing protocols such as AODV establish routes only when needed, by flooding a Route Request (RREQ) and letting the destination (or an intermediate node with a fresh route) reply with a Route Reply (RREP). This design is efficient, but it assumes that the path a RREP describes reflects a real, physical sequence of hops. The wormhole attack breaks that assumption without needing to compromise any node's cryptographic keys or forge any packet content: two attacker-controlled nodes simply capture traffic at one location and re-inject it at another, over a private channel (a wired link, a directional antenna, or an out-of-band wireless channel) that is faster or more direct than the multi-hop path it is impersonating. Because the packets themselves are unmodified and authentic, standard authentication and encryption do nothing to stop it.

The practical effect is that routes running through the wormhole look shorter and faster than legitimate alternatives, so ordinary shortest-path route selection favors them. Once enough traffic is drawn through the wormhole, the attackers gain the ability to eavesdrop, selectively drop packets (turning the wormhole into a black hole at will), or destabilize the network by repeatedly breaking and re-forming the illusory route. This paper's goal is to propose a detection approach that (a) does not require special hardware such as GPS or directional antennas, (b) does not require tight clock synchronization across the network, and (c) tolerates the natural noise of a mobile, wireless environment well enough to avoid flagging every network hiccup as an attack.

2. RELATED WORK

Wormhole defenses in the literature generally fall into a few families, each with a different cost profile.

2.1 Packet Leashes and Timing-Based Methods

Hu, Perrig, and Johnson introduced the wormhole attack formally and proposed packet leashes as a defense: a geographic leash restricts how far a packet could plausibly have travelled using location information, while a temporal leash restricts it using tightly synchronized timestamps and an authentication protocol (TIK) [1]. This work established the core insight that a wormhole tunnel, however fast, still has to violate either the physical distance a packet could travel or the time it should take to do so — but the geographic variant needs location hardware, and the temporal variant needs precise clock synchronization, both of which are costly to guarantee on ordinary mobile devices.

2.2 Guard-Node and Neighbor-Monitoring Methods

Khalil, Bagchi, and Shroff proposed LITEWOP, a lightweight scheme in which guard nodes monitor their neighborhood's control traffic to detect inconsistent link claims without needing clock synchronization or special hardware [2]. Its main limitation is that once a wormhole is detected, the network is simply left aware of it rather than actively repaired, which the same authors later addressed with a follow-up protocol that removes malicious nodes through a coordinating authority [10].

2.3 Hardware-Assisted and Location-Based Methods

Hu and Evans proposed using directional antennas so that a node can verify a neighbor's claimed direction, catching wormholes that rely on presenting fake neighbor relationships, though this approach depends on specialized antenna hardware that is not standard on typical mobile devices [3].

2.4 Graph-Theoretic and Statistical Methods

Poovendran and Lazos developed a graph-theoretic framework that models the conditions under which a network topology can or cannot be protected against wormhole placement, offering a more formal way to reason about detectability but requiring assumptions about network deployment that do not always hold in a mobile setting [4]. Separately, statistical approaches such as that of Song, Qian, and Li analyze the distribution of round-trip times across multiple paths to flag routes that are anomalously fast compared to the rest of the network, without needing GPS or synchronized clocks [5].

2.5 Hop-Count and Delay-Per-Hop Methods

Chiu and Lui's DelPHI mechanism compares delay-per-hop values across multiple disjoint paths to the same destination, flagging paths whose delay-per-hop is implausibly low [6]. Jen, Lai, and Kuo proposed a hop-count analysis scheme built on the observation that a wormhole artificially shortens the hop-count reported for a route relative to what the network's real diameter and density would suggest [7]. These hop-count and delay-based approaches are attractive because they need no extra hardware, but used alone they are vulnerable to being confused by ordinary topology changes as nodes move.

Table 1 — Comparison of representative wormhole defenses discussed above (organizational summary, not experimental data).

Method	Core signal used	Needs GPS / clock sync?	Needs special hardware?	Main limitation
Packet Leashes [1]	Geographic distance or authenticated timestamp	Yes (either location or tight sync)	GPS for geo-leash	Costly to guarantee on commodity devices
LITEWOP / MOBIWOP [2, 10]	Guard-node monitoring of neighborhood control traffic	No	No	Detection-only unless paired with removal protocol
Directional antennas [3]	Verified direction of neighbor's signal	No	Yes (directional antenna)	Requires non-standard antenna hardware
Graph-theoretic framework [4]	Topology feasibility analysis	No	No	Relies on deployment assumptions not always true on mobile nets
Statistical RTT analysis [5]	Distribution of RTTs across multiple paths	No	No	Needs enough alternate paths to compare against
DelPHI [6]	Delay-per-hop across disjoint paths	No	No	Requires multiple disjoint paths to exist
Hop-count analysis [7]	Hop-count vs. expected network diameter/density	No	No	Can be confused by genuine short routes
TARH (this proposal)	Hop-count plausibility + RTT/hop-count consistency + trust accumulation	No	No	Design-stage; not yet validated by simulation

2.6 Gap Motivating This Proposal

Across this body of work, a consistent trade-off appears: hardware- or synchronization-dependent methods (packet leashes, directional antennas) tend to be more precise but harder to deploy on commodity devices, while lightweight, hardware-free methods (hop-count analysis, statistical RTT analysis) are

easier to deploy but more prone to false positives under normal mobility. This paper's proposal is positioned in the second category, but it tries to reduce the false-positive risk of a single lightweight signal by combining two independent signals with a trust mechanism that requires a repeated pattern of suspicious behavior before a node is treated as an attacker.

3. PROBLEM STATEMENT

A wormhole route has two properties that are difficult for the attacker to fully disguise at once. First, its reported hop-count is usually lower than what the physical distance between source and destination, combined with the network's typical node density and radio range, would predict — the tunnel effectively erases hops that should have been necessary. Second, the round-trip time observed for that route often does not scale with hop-count the way ordinary multi-hop paths do, either because the tunnel link is unusually fast (making RTT too low for the claimed hop-count) or because processing and re-encapsulation at the tunnel endpoints adds a fixed delay that does not resemble typical per-hop forwarding delay (making the RTT pattern irregular rather than roughly linear in hop-count).

Relying on either signal alone is fragile: hop-count can look artificially low simply because a real short route happens to exist in a dense area of the network, and RTT is naturally noisy in wireless environments due to contention, retransmission, and node mobility. The problem this paper addresses is how to combine these two individually noisy but structurally different signals, together with an accumulating notion of trust per neighbor, so that detection stays sensitive to genuine wormholes while remaining tolerant of the topology changes and timing jitter that are normal in a mobile network.

4. PROPOSED SYSTEM

The proposed scheme, referred to here as Trust-Aware RTT/Hop-Count Detection (TARH), extends AODV's route discovery process with three cooperating components: a hop-count plausibility check, an RTT-versus-hop-count consistency check, and a per-neighbor trust score that governs how strongly any single suspicious observation affects a node's standing.

4.1 Hop-Count Plausibility Check

Each node maintains a rolling estimate of the average one-hop neighbor density and radio range in its vicinity, built from the neighbor lists it already exchanges as part of normal routing (e.g., via Hello messages). From this, a node can derive a rough expected minimum hop-count for a route of a given estimated source-destination separation. When a

RREP arrives reporting a hop-count that falls well below this expected minimum for the distance implied by the request, the route is marked as hop-count-suspicious. This check deliberately uses a soft, density-derived expectation rather than a fixed global constant, so that it adapts as nodes move into denser or sparser regions of the network.

4.2 RTT-versus-Hop-Count Consistency Check

Independently, the source node measures the round-trip time between sending a RREQ and receiving the corresponding RREP, and compares it against the RTT that would be expected for the reported hop-count, based on a locally maintained running average of per-hop delay observed on the node's other, already-validated routes. Two anomaly patterns are treated as suspicious: an RTT substantially lower than expected for the claimed hop-count (consistent with a fast out-of-band tunnel), and an RTT that does not track hop-count consistently across repeated route discoveries to the same destination (consistent with a fixed tunnel-endpoint processing delay rather than genuine per-hop forwarding). A route is marked RTT-suspicious if either pattern crosses a locally-adaptive deviation threshold, expressed in terms of the node's own recent RTT variance rather than a fixed global value, again to tolerate the natural jitter of wireless links.

4.3 Per-Neighbor Trust Score

Neither check alone marks a node as malicious. Instead, every node maintains a trust score for each neighbor that forwards a RREP on its behalf, initialized to a neutral value. Each time a route through a given neighbor is marked hop-count-suspicious or RTT-suspicious, that neighbor's trust score is decremented; each time a route through that neighbor completes normally and the corresponding data transfer proceeds without anomalies (e.g., without an unusually high drop rate, which could indicate the wormhole has been converted into a black hole), the trust score is incremented, subject to a ceiling. Trust scores decay slowly toward the neutral value over time when no new observations are made, so that a node which stops behaving suspiciously — or a false accusation based on a stale observation — does not permanently condemn a neighbor. A node whose trust score crosses a low-trust threshold is excluded from future route selection and is announced to the surrounding neighborhood as a candidate wormhole endpoint, prompting other nodes to weight their own trust scores for that node downward as well, so that corroborating evidence from multiple independent observers propagates faster than any single node's opinion could.

4.4 Overall Detection Flow

When a source node receives a RREP, it evaluates the hop-count plausibility check and the RTT consistency check independently. If neither check flags the route, the route is accepted normally. If exactly one check flags the route, the associated neighbor's trust score is decremented but the route is still tentatively usable, since a single ambiguous signal is treated as weak evidence given how noisy either signal can be alone. If both checks flag the same route, the neighbor's trust score is decremented more sharply and the route is deprioritized in favor of an alternative, if one exists. Only sustained low trust — accumulated either from repeated single-signal flags or from a smaller number of double-signal flags — results in a neighbor being excluded from routing and reported to the wider neighborhood. This graduated response is intended to make the system resistant to a single unlucky combination of mobility and contention producing a false alarm, while still converging quickly on a genuine, persistently-misbehaving wormhole pair.

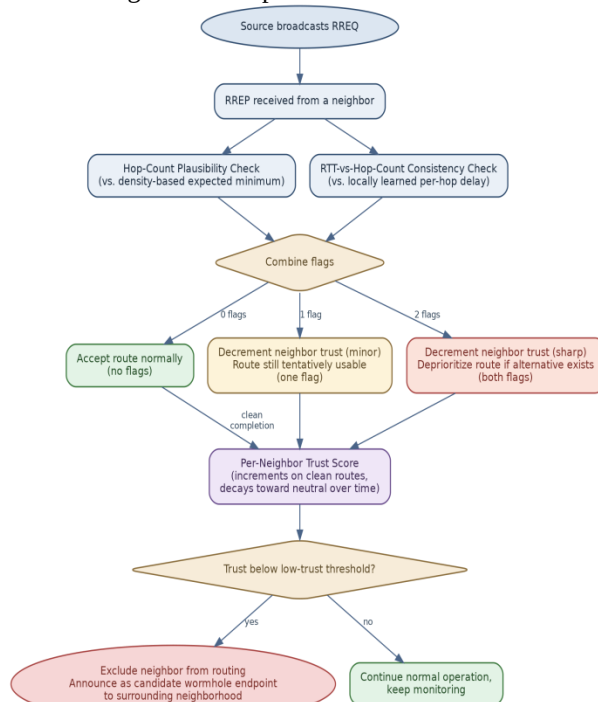


Figure 1 Tarh Detection Flow: Hop-Count And Rtt Checks Feed A Combined Flag Decision, Which Updates A Per-Neighbor Trust Score; Sustained Low Trust Triggers Exclusion And Neighborhood-Wide Announcement.

4.5 Design Parameters

The parameters below are named and described symbolically rather than given tuned numeric values, since no simulation has been run to calibrate them; Section 6 outlines how they would be tuned.

Table 2 — Tarh Design Parameters (Symbolic; To Be Tuned During Future Evaluation).

Parameter	Meaning	Where used
θ_{hop}	Minimum-hop-count deviation tolerance relative to the density-based expectation	Hop-count plausibility check (4.1)
θ_{rtt}	Allowed RTT deviation from expected value, expressed in units of local RTT variance	RTT consistency check (4.2)
$\Delta_{\text{trust}}(1)$	Trust decrement applied for a single-signal flag	Trust update, weak case (4.3, 4.4)
$\Delta_{\text{trust}}(2)$	Trust decrement applied when both signals flag the same route	Trust update, strong case (4.3, 4.4)
Δ_{trust}^+	Trust increment applied for a clean route completion	Trust update on success (4.3)
λ_{decay}	Rate at which trust decays back toward the neutral value when no new observations occur	Trust decay over time (4.3)
T_{low}	Low-trust threshold below which a neighbor is excluded and announced	Exclusion decision (4.3, 4.4)
W_{density}	Window size (time or sample count) used to estimate local neighbor density	Hop-count expectation model (4.1)

5. DISCUSSION: EXPECTED BEHAVIOR AND TRADE-OFFS

Because TARH is presented here at the design level, this section describes the trade-offs the design is intended to manage, rather than reporting measured outcomes.

Detection sensitivity vs. false positives: combining two structurally different signals is intended to reduce false positives relative to either check used alone, since a genuine topology change is unlikely to simultaneously produce both an implausibly low hop-count and an inconsistent RTT-to-hop-count pattern, whereas a real wormhole tends to produce both.

Convergence delay vs. stability: the trust-decay design trades a slower response to a first suspicious observation for greater stability against transient noise; this delay would need to be tuned against how quickly a real wormhole can do damage once traffic is drawn to it.

Overhead: the scheme reuses information nodes already exchange (Hello messages, RREQ/RREP

timing) and adds only local bookkeeping (trust scores, running RTT/hop-count averages) rather than new control packets, which should keep bandwidth overhead low, though the exact CPU and memory cost per node would need to be measured on representative hardware.

Colluding-attacker resistance: because trust judgments are also shared as neighborhood announcements, an isolated wormhole pair should be easier to corner than in a purely local, per-node detection scheme; a network with many colluding malicious nodes would stress this assumption and is a natural stress-test scenario for future evaluation.

6. SUGGESTED EVALUATION METHODOLOGY (FUTURE WORK)

No experiments have been run for this proposal; the following is a description of how it would be validated, intended as a starting point for future implementation work rather than a report of results.

Simulation platform: a discrete-event network simulator supporting AODV (e.g., NS-2/NS-3 or a comparable tool) with the ability to inject a configurable wormhole tunnel between two designated malicious nodes.

Independent variables: number of wormhole node pairs, node mobility speed and model, network density, and background traffic load.

Metrics: detection rate and false positive rate for the wormhole nodes specifically, packet delivery ratio, end-to-end delay, and routing control overhead, each compared against plain AODV (no defense) and against at least one prior scheme such as a hop-count-only or RTT-only baseline, to isolate the benefit of combining the two signals.

Sensitivity analysis: the trust-score increment/decrement/decay parameters and the adaptive deviation thresholds should be varied to characterize the sensitivity-vs-stability trade-off described above, rather than reported as a single fixed configuration.

CONCLUSION

This paper proposed TARH, a hardware-free, synchronization-free detection approach for wormhole attacks in MANETs that combines a density-adaptive hop-count plausibility check with an RTT-versus-hop-count consistency check, mediated by a slowly-decaying per-neighbor trust score. The approach is designed to address a specific gap identified in prior work: lightweight, hardware-free detection signals tend to be individually noisy in mobile settings, and this proposal's central idea is that requiring corroboration across two structurally different signals, accumulated over time rather than judged from a single observation, should reduce false

positives without sacrificing the ability to catch a persistent wormhole. As presented, this is a design proposal rather than a validated result, and the paper explicitly separates its architecture description from the evaluation plan needed to test it. Future work is to implement TARH in a network simulator, tune its trust and threshold parameters, and compare it quantitatively against the timing-based, guard-node, and hop-count baselines discussed in the related work section.

REFERENCES

- [1]. Hu, Y.-C., Perrig, A., Johnson, D. B. "Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks." IEEE INFOCOM, 2003 (journal version: Wormhole Attacks in Wireless Networks, IEEE JSAC, 2006).
- [2]. Khalil, I., Bagchi, S., Shroff, N. B. "LITEWOP: A Lightweight Countermeasure for the Wormhole Attack in Multihop Wireless Networks." International Conference on Dependable Systems and Networks (DSN), 2005.
- [3]. Hu, L., Evans, D. "Using Directional Antennas to Prevent Wormhole Attacks." Network and Distributed System Security Symposium (NDSS), 2004.
- [4]. Poovendran, R., Lazos, L. "A Graph Theoretic Framework for Preventing the Wormhole Attack in Wireless Ad Hoc Networks." ACM/Springer Wireless Networks, 2007.
- [5]. Song, N., Qian, L., Li, X. "Detection of Wormhole Attacks in Multi-Path Routed Wireless Ad Hoc Networks: A Statistical Analysis Approach." IEEE International Parallel and Distributed Processing Symposium (IPDPS), 2005.
- [6]. Chiu, H. S., Lui, K.-S. "DelPHI: Wormhole Detection Mechanism for Ad Hoc Wireless Networks." International Symposium on Wireless Pervasive Computing, 2006.
- [7]. Jen, S.-M., Lai, C.-S., Kuo, W.-C. "A Hop-Count Analysis Scheme for Avoiding Wormhole Attacks in MANET." Sensors, 9(6), 2009.
- [8]. Wang, W., Bharghavan, B., Lu, Y., Wu, X. "Defending against Wormhole Attacks in Mobile Ad Hoc Networks." Wireless Communications and Mobile Computing, 2006.
- [9]. Buttyán, L., Dóra, L., Vajda, I. "Statistical Wormhole Detection in Sensor Networks." European Workshop on Security in Ad Hoc and Sensor Networks (ESAS), 2005.
- [10]. Khalil, I., Bagchi, S., Shroff, N. B. "MOBIWOP: Mitigation of the Wormhole Attack in Mobile Multihop Wireless Networks." Ad Hoc Networks, 6(3), 2008.