THE INTERNATIONAL JOURNAL OF SCIENCE & TECHNOLEDGE

Wormhole Avoidance Using Reputation-Based Routing

N. Kusuma
Assistant Professor, Malla Reddy Institute of Technology and Science, Hyderabad, India

Abstract:
A novel routing protocol is presented (reputation-based routing) which attempts to avoid wormholes via the topologies in which attackers will take time to deploy their wormhole. Simulation results demonstrate its avoidance performance advantages in a variety of topologies. A reputation-based routing approach is introduced, drawing insights from reinforcement learning, which retains routing decisions from an earlier stabilisation phase.
Results again demonstrate favourable avoidance properties at a reduced energy cost. A cross-layer approach physical reputation based routing which feeds physical-layer information into the reputation-based routing algorithm is presented, permitting candidate routes that make use of the best beamforming relays to be discovered.

Key words*: Reputation-based Routing(RBR),wormhole, topology*

1. Introduction

This paper presents an wormhole avoidance approach, reputation-based routing (RBR), which is viable in topologies in which attackers will take time to deploy their wormhole. A logarithmic reputation metric is demonstrated to create long- term memory in the network that encourages reuse of nodes and links traversed earlier, favouring the use of wormhole free paths even after a shortcut across the network is introduced by a wormhole attacker. Simulation results are presented to verify the performance of the reputation-based routing approaches.

Reputation-based routing is chosen to provide a viable wormhole avoidance approach in scenarios in which it can be assumed that a stabilization interval free of attack exists. This is likely to be the case, for example, in scenarios in which the attacker is assumed to be poorly resourced, or a deployment is spontaneous. The reputation- based routing approach has the advantage of not requiring tunable parameters such as the α and β values involved in the disturbance-based routing schemes. This absence of parameters simplifies deployment by removing the requirement to consider tuning the scheme to specific topology characteristics, which therefore improves the simplicity of deployment. This paper motivates the intuitions behind the novel reputation-based routing approach [1], defines its metric and logic of operation, and presents simulation results to demonstrate its performance characteristics for standard topologies.

2. Overview of Reputation-Based Routing

The nature of the novel idea, reputation-based routing, presented in this paper is to provide routing that is resilient against the future introduction of a wormhole attack via a conceptually simple and persistent reputation metric, updated and reinforced by the dynamic traffic patterns at a particular node. In this section the nature of the idea and its protocol operation will be defined and design consequences explored. The goal of the approach is to introduce long-term hysteresis into routing decisions, in which even though particular routes have expired, their constituent nodes remain favoured candidates for later routing by the rest of the network.

The key idea is that in many attack scenarios there can be expected to be a stabilization interval from early deployment, during which the network will remain free of threats. In a newly deployed network, before implementing a wormhole attack, the attacker would be required to scan the topology, locate the sink, determine the goals of the network, realize that a wormhole is the desired attack vector to gain control of network routing, and implement their attack.

It can be assumed that this stabilization interval will form a safe operational window during which the network can operate unhindered, particularly if node deployment is a gradual process and nodes self-organize to discover routes from their individual activation. Within this interval, the nodes will perform their routing and data dissemination along wormhole-free paths, loading the reputation metrics such that these nodes become preferential nodes for inclusion in routes.

The protocol depends entirely on local calculations using overheard information as part of the normal routing process. As a result, it does not impose any additional overheads as seen in other wormhole detection mechanisms. Potential overheads include sentry packets as in packet leashing or watchdog packets for collaborative behaviour checking[2].The underlying logic of the routing protocol can operate using a standard and well-tested routing protocol for end-to-end metric minimization such as AODV[3].This assists integration of the protocol into existing sensor network operating systems, allowing it to use similar routing logic but with a custom metric.

3. Philosophy Behind Reputation-Based Routing

Consider the case in which an attacker deploys a wormhole some time after the network begin operation. Previously, it can be anticipated that routing protocols carrying traffic to the sink would have taken relatively direct routes. However, when the wormhole is introduced, the topology is suddenly changed dramatically, with the wormhole presenting a shortcut across several hops. If a routing metric can be devised in which the previous usage of those hops creates a sufficiently powerful incentive to continue using them in the presence of the sudden topology change, then the wormhole attack will fail to draw significant traffic. Figure 1 illustrates this, demonstrating the accumulation of reputation in the early phases of operation that later leads those nodes to be preferred over a newly introduced wormhole shortcut with no reputation.

The intuition behind the reputation routing protocol is to create suspicion regarding topology changes and a resulting disincentive to use the newly available shortcut route that a wormhole would introduce. The reputation metric is structured so that even though the original routes have expired and the wormhole now provides a shortcut route to the destination, the newly established wormhole and its surrounding nodes do not have sufficient reputation to be selected. Thus,the reputation-based routing protocol will treat these new routes with suspicion and will favour the routes featuring trusted nodes until the alternatives are exhausted.

The previous section an overview of reputation-based routing metric. During the stabilization interval, reputation levels have incremented upon nodes on the route shown at the start of the sink. When the wormhole is introduced, the nodes around its endpoint do not have sufficient reputation for the route through the wormhole to be chosen for routing. Therefore, the safe route continues to be located.

3.1. Reputation Metric Definition

Given a particular multihop route in the network, successful delivery of data to an endpoint requires retransmission at all intermediate nodes along the route. If a node is malicious and refuses to forward, or is subjected to destructive jamming interference or the presence of a wormhole, then the route carries an increased probability of failure. The challenge for an avoidance protocol is to determine the probability that a wormhole or other security threat is located within a region. It is possible to explore the use of an analytic approach, in which a priori information about the structure and nature of an attack is explored to the individual link probabilities.

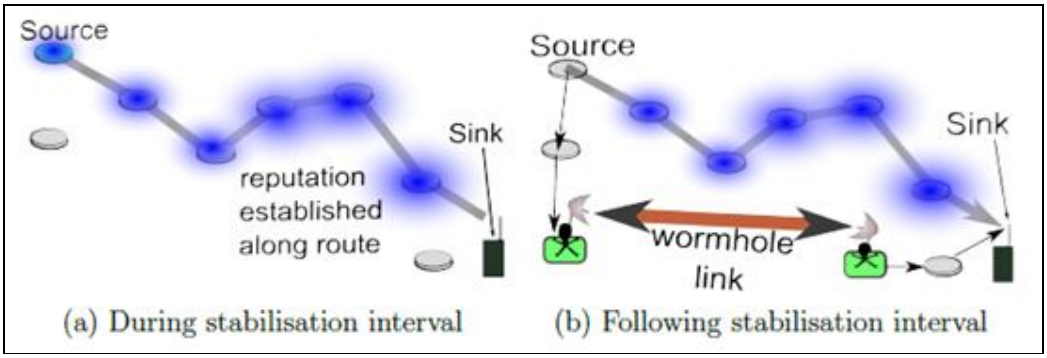

Figure 1: Operation of reputation based routing, preferring long-established routes

However, in order to make the best selection of routes in an operating network in which the precise form of the attack is unknown and no statistical assumptions about the placement of wormholes help to structure the attack, a more robust mechanism will use empirically sampled past performance to approximate these probabilities. Therefore an estimate of the likelihood of routing success can be obtained from historical information, using the concept of a per-node reputation level $RLEVEL_i$. This represents the reputation, and an aggregate of the trust placed in a node from its successful forwarding. RLEVEL itself is bounded to one, a state that represents complete trust of a particular node. Complete trust occurs when the bandwidth demand of the route replies received is equal to the node response.

The reputation level of a single node is increased on each successful routing response unicast back from the sink by RLEVEL_INC, which is defined for new route R by Equation 1.1 in terms of the bandwidth demand of the particular route BWR (its data rate request carried in a routing header) and the data rate DRi of the transceiver at Ni.

$$RLEVEL\_INC(R) = \frac{BWR}{DRi} \quad (1.1)$$

The reputation metric of a single link between nodes N_i and N_j , RMi;j is defined as a function of the reputation level of the originator at that particular time t, $RLEVEL_i(t)$, in Equation 1.2. The reputation metric is initialised to a nominal reputation null constant (RNK) upon activation of the protocol. Therefore for formation of the first route (before any reputation increments are received) the behaviour of the protocol is effectively equivalent to shortest-path routing. The nature of the logarithmic function employed is that as $RLEVEL_i$ tends to one, the reputation metric of the nodes upon the path to the sink goes to zero.

$$RM_{i,j}(t) = \begin{cases} RNK & \text{if } RLEVEL_i(t) = 0 \\ -ln(RLEVEL_i) & \text{if } RLEVEL_i(t) > 0 \end{cases} \quad (1.2)$$

A node with data to transmit that does not have an active route to the sink, broad- casts a RBR-RREQ, which is retransmitted at intermediate nodes, incrementing the aggregate reputation metric stored in the packet as it travels. Upon receiving a new reputation-based routing request, the sink chooses the end-to-end route with the lowest aggregate reputation metric (representing the highest reputation levels and thus the best choice), and unicasts the reply along the reverse route which serves to increment the reputation level.

From this, routes featuring nodes with a high RLEVEL (which have previously carried large amounts of traffic) will be rewarded strongly. The effect of this is to make the reputation algorithm very cautious, biasing it heavily towards the use of previously explored nodes, with a high reputation level, wherever possible. This is precisely the effect desired to engineer a secure network.

4. Simulation Methodology and Validation

4.1. Scenario Definition

This section defines the simulation scenarios, which are designed to model a security- critical hypothetical military deployment. The scenarios considered consist of a fixed region of terrain, within which the network operator seeks to defend their territory and track the motion of hostile enemy troop groupings. Homogeneous detection nodes are arranged within this region, using the standard topologies of Radial Ring based and grid-based . This ensures that topologies employed are representative of a wide variety of network situations, in which terrain prohibits an optimal regular deployment

For the grid-based scenarios, the sink is located at the military headquarters upon the northern edge of the topology. For the radial ring topologies, the sink is located centrally. The malicious attacker chooses to deploy one of their wormhole endpoints within a one-hop distance from the sink. The remote pickup endpoint of the wormhole is located upon the midpoints of either the southern edge of the topology.

In this scenario it is assumed that, immediately following the stabilization interval, the attacker activates their wormhole. This could either occur by the deployment of the endpoints, or the activation of the link between them. Following this, future routing packets and responses are tunneled through the wormhole, which allows allow it to control routing as usual in the case of an attack.

Armies move in a randomly selected direction, reacting of the boundaries of the southern half of the deployment region. At the new ow interval on approach of an army within detection range of an idle detection node, routing to the sink is initiated according to the defined protocol. Network routing is updated at each routing interval, and rows remain active at their given ow rate for their specified route lifetime. During simulation, the wormhole is activated after the stabilization interval, and then begins to propagate traffic as intended. The simulation is implemented as a custom program in the OCaml programming language.

4.2. Simulation Methodology

The simulator generates an ensemble of topologies. In each topology, connectivity between nodes is modelled according to a standard protocol model, assuming bidirectional binary connectivity within a given peer distance threshold P_R. This assumes that a link is connected if its endpoints lie within the range P_R, and disconnected if they are outside of this. For simplicity, the maximum sensing range S_R within which the nodes will detect troops, is set equal to the communication range. Periodically, at the new ow interval during simulation, the fresh position of each troop cluster is recomputed using their known velocity, previous position, and the time delay. The simulator checks for idle sources surrounding each troop cluster within S_R, and proceeds to activate the nearest idle source for reporting. Reputation level increments are applied to the route with the lowest aggregate metric.

4.3. Success Metric Definition

The metric employed to analyze reputation-based routing is the avoidance advantage ADV. The simulator records a metric to assess the success of reputation-based routing with the given topology properties. The avoidance advantage (ADV) is the additional proportion of all discovered routes throughout the simulation that successfully avoid the wormhole under the disturbance scheme as compared to shortest path. A value of zero corresponds to a state in which the disturbance- based scheme delivers no advantage, as precisely the same proportion of routes used the wormhole as in shortest path routing.

4.4. Simulation Validation

This section considers validation of reputation-based routing simulations. The core of reputation routing simulation is based upon the software developed for disturbance-based routing, and therefore inherits the tests for the routing and results generation.

4.5. Single Circle Topology for Reputation-Based Routing Validation

This section will consider a simple single circle topology, and the behaviour of the reputation-based routing protocol within it. Simulation behaviour will be compared against an analytic model to verify correct computation of the reputation-based routing metrics with additional routes, and correct routing decisions according to the protocol logic.

Consider a simple topology as depicted within Figure 2 . This circular test topology contains C = 16 uniformly spaced nodes around the circle, with the sink node as one of them with index N_1. The connectivity of the topology is sufficient to connect all

adjacent nodes within the circle. Node N_2 is originally disabled. As a result the data transmissions from node N_3 at the start of network activation must form a multihop route counter-clockwise all the way around the circle.

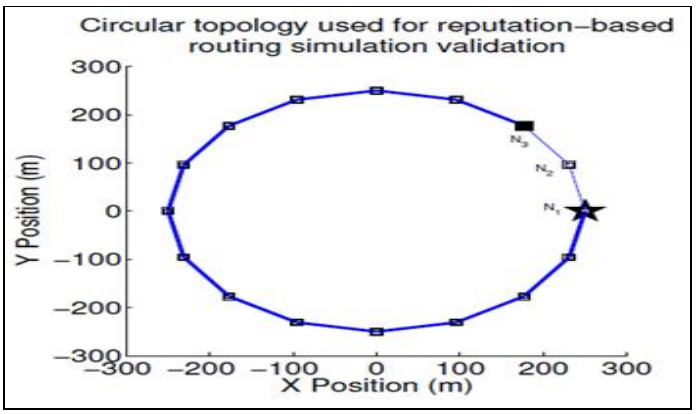

Figure 2: The circular test topology

4.6. Validating Reputation-Based Routing Against Analysis

After a given time interval T_{change}, disabled node N_2 is activated. This models the process by which a wormhole changes the connectivity properties of the system. A potential shortcut is now available in which node N_3 is connected to the sink via an intermediate clockwise hop through N_1. In order to provide wormhole avoidance, reputation-based routing should however choose to reject the shortcut in favour of the previous counterclockwise route. This occurs when sufficient reputation has accrued for the route to have a lower overall reputation metric, despite its overall increased length.

Upon its initialisation, the node N_2 upon the newly introduced shortcut does not have any reputation, and therefore the metric for the hop using it is the reputation null constant RNK (Equation 1.2). Since only the intermediate hops and not the originator itself contribute to the reputation metric, the shortcut route metric only contains the contribution from the link leaving N2. For a reputation level $RLEVEL_{min}$ at which the previous counterclockwise route will be equal in aggregate metric to the shortcut, the following must hold:

$$RNK = -\sum_{i=4}^{C} ln(RLEVEL_{min}) \quad (1.3)$$

The reputation upon all previously used nodes will be a constant, due only a single source N_3 being previously activated. Therefore the summation can be replaced with the number of nodes contributing to the reputation. This gives the following relationship between the parameters:

$$RNK = -(C-3)ln(RLEVEL_{min}) \quad (1.4)$$

In order to verify this relationship, the simulation results were contrasted with this analytic prediction. The simulation proceeded by generating the previously described circular topology, with N_2 adjacent to the sink disabled. Given a reputation level target and a particular value of the null constant RNK, initial routes were formed until the reputation level equalled this value. At this point, the disabled node was reactivated to offer a shortcut route. Success was recorded for the trial if the counter- clockwise route was used, and failure if the shortcut was used. Figure 3 shows an example of failure and successful cases during this routing operation. In the successful avoidance case, K = 10 and RLEV EL = 0:5, which is, as predicted analytically, sufficient reputation to continue using the counter-clockwise route. In a failure case, K = 10 and RLEV EL = 0:4.

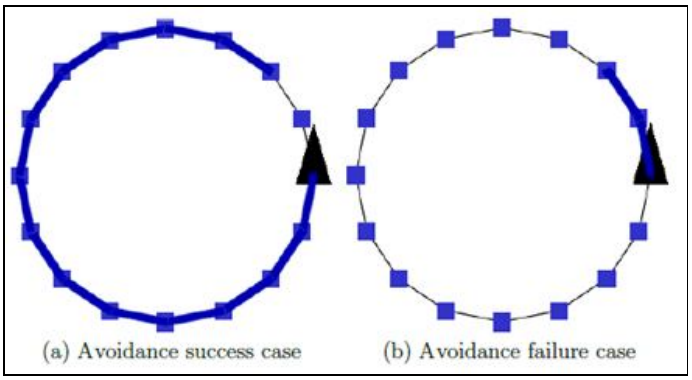

Figure 3: Simulation of reputation-based routing in the simulation test topology

analytically predicted values. This validation test is conducted in a single circle topology consisting of C = 16 nodes (including the sink as N_1). The figure shows the minimal value of RNK which allowed the reputation-based routing protocol to successfully use its original route in the presence of the shortcut. This was found using a bisection method, beginning with a range of RNK values from 0 to 50.

This range was iteratively bisected and the midpoint tested, to discover the smallest value of RNK that produced successful avoidance of the shortcut. It is clear that the simulation results for minimal required RNK are precisely as predicted by the equation. This serves as validation of the simulator logic for route establishment and computation of the reputation metrics.

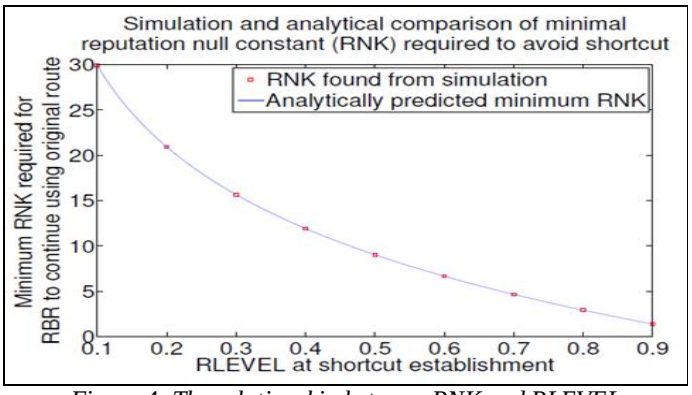

Figure 4: The relationship between RNK and RLEVEL

4.7. Default Parameters

Unless otherwise specified, the parameters displayed in Table 1 are employed to generate the full simulation results for this paper

5. Results

This section describes and analyses the performance of reputation-based routing in ensembles of grid-based Gaussian, radial ring and uniform random topologies The results use a stabilisation interval of S_i=200 seconds, corresponding to the lifetime of 20 routes. Following the stabilization interval, the wormhole is deployed and activated by the attacker. The wormhole remote pickup endpoint is located at a fixed location in the midpoint of the southern edge or eastern edges of the topology. These correspond to the cases in which the attacker controls a fixed edge region of the topology far from the sink and is able to install their wormhole in this region.

Parameter	Symbol	Default Value
Simulation run topology ensemble size		50
Simulation runtime		3000 seconds
Stabilisation interval	S_i	200 seconds
Routing interval		10 seconds
Route lifetime		100 seconds
Bandwidth demand	BW_R	$5kbit/s$
Channel data rate	DR	$250kbit/s$
Grid based Gaussian regularity factor	R_f	0.9
Topology edge size	S	1000m
Peer communication distance	P_R	150m
Grid based Gaussian node count	N	100
Radial topology ring count	R_{MAX}	6
Radial topology ring separation	s	100 (m)
Radial topology radian separation	k_r	0.9

Table 1: Default parameters employed in simulation results

Figure 5 illustrates the avoidance advantage provided by the reputation- based routing scheme in the described scenario across an ensemble of 50 topologies. These results are presented as a cumulative distribution function to allow the range of avoidance advantage values across the ensemble of topologies to be examined and any outlier results identified. The performance for the highly regular topologies is very consistent. For the wormhole located upon the southern edge in grid-based Gaussian topologies, the median avoidance advantage is 0:97, and for the radial ring topology it is 0:87. Reputation-based routing always delivers an avoidance advantage above 0:8 in the case of southern wormhole placement in the grid-based and radial topologies.

The grid-based Gaussian topology result is considerably better than that achieved by the dynamic disturbance-based routing scheme. With edge wormhole placements, the best avoidance advantages generated in the grid-based Gaussian topology were below 0:4. Therefore, reputation-based routing can deliver twice the avoidance advantage of dynamic disturbance in this regular topology. This is due to the reputation buildup during the stabilization phase across these highly regular topologies, which create tendencies to use these stable routes again from any nodes in the network.

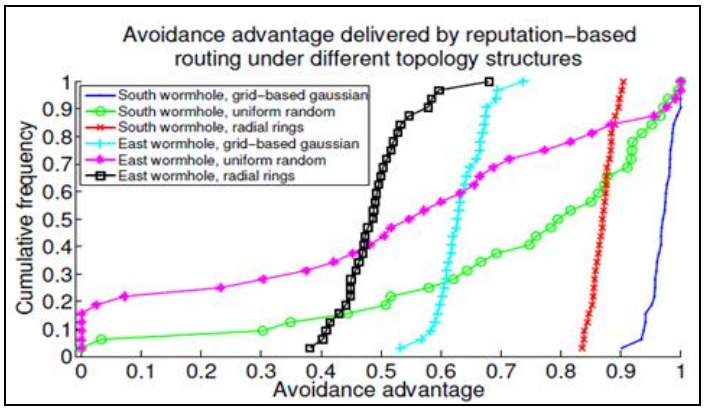

Figure 5: Distribution of avoidance advantage for reputation routing, under various topology ensembles

For both wormhole placements, in the uniform random case there are some cases in which reputation-based routing fails to deliver such consistent performance. These have been investigated and shown to be those in which the local connectivity properties disadvantage the wormhole under the metric chosen. For example, the avoidance advantage metric is defined relative to how many routes would use the wormhole anyway under shortest path. If the wormhole placement site is poorly connected within the topology graph and thus offers an unfavourable shortcut, it may not achieve an advantage since it may be unreachable under either shortest path or reputation-based routing. This is not however a security failure, as the attackers will fail to achieve a significant gain from their wormhole.

This highlights a potential issue for deployment of reputation-based routing in irregular topologies. If the topology is sufficiently irregular that all traffic is bridged under a single link, then it is likely that introducing a wormhole next to this link could hijack its reputation. Therefore a condition for deployment of the scheme is that, if randomly deployed, the topology must guarantee sufficient connectivity along a variety of redundant paths (beyond the requirement for mere reachability of all nodes from the sink) to ensure an effective flow of reputation to the sink.

6. Conclusion

This paper has introduced reputation-based routing, the motivation behind its introduction, and the logic that allows it to successfully avoid wormhole attack introduced after a given stabilization interval, via its hysteresis which causes it to favour previously established routes for future routing following their expiry. Simulation results have demonstrated the performance of reputation-based routing, showing a high avoidance advantage in topologies in which wormholes exist at a fixed location. It has been shown that the scheme is capable of operating successfully at schemes with a short stabilization value. As long as the network as deployed can achieve full connectivity across a variety of diverse paths, implying that the topology must be sufficiently regular, reputation-based routing can avoid wormholes with high probability.

7. References

1. J. Harbin, P. Mitchell, and D. Pearce, Wireless sensor network wormhole avoidance using reputation-based routing in ISWCS 2010: Seventh International Symposium on Wireless Communication Systems, {525, Sept. 2010}.
2. S. Marti, T. J. Giuli, K. Lai, and M. Baker, Mitigating routing misbehavior in mobile ad hoc networks in ACM MobiCom 2000: Proceedings of the 6th International Conference on Mobile Computing and Networking,{265, ACM, 2000}.
3. C. Perkins and E. M. Royer, Ad-hoc On-Demand Distance Vector (AODV) Routing in IEEE Workshop on Mobile Computer Systems and Applications, vol. 100, pp. 90{100, Feb. 1999}.
4. Y. C. Hu, A. Perrig, and D. B. Johnson, "Packet leashes: a defense against wormhole attacks in wireless networks," IEEE Computer and Communications Societies. IEEE, vol. 3, pp. 1976-1986, 2003.
5. W. Wang and B. Bhargava, "Visualization of wormholes in sensor networks," in Proceedings of the 3rd ACM workshop on Wireless security. ACM New York, NY, USA, 2004, pp. 51-60