A Current Review on Using Directional Antennas to Prevent Wormhole Attacks

Srinivas Ambala, Research Scholar, Sunrise University, Rajasthan
Guide Name: Dr., Sudhir Dawra, Supervisor, Sunrise University, Rajasthan

Abstract

Wormhole assaults empower an aggressor with restricted assets and no cryptographic material to wreak devastation on remote systems. To date, no broad resistances against wormhole assaults have been proposed. This paper introduces an examination of wormhole assaults and proposes a countermeasure utilizing directional antennas. We display an agreeable convention whereby hubs share directional data to keep wormhole endpoints from taking on the appearance of false neighbors. Our safeguard extraordinarily reduces the danger of wormhole assaults and requires no area data or clock synchronization.

1. Introduction

Remote specially appointed systems have properties that expansion their helplessness to assaults. Remote connections are characteristically helpless against listening stealthily and message infusion, and in addition sticking assaults. Requirements in memory, processing force, and battery control in cell phones can force exchange offs amongst security and asset utilization.

Directing in specially appointed remote systems is a particularly hard undertaking to fulfill safely, heartily and proficiently. Many proposed directing conventions are centered around vitality, and give no insurance against an enemy. Some protected steering conventions additionally have been proposed.

Notwithstanding, because of the eccentrics of impromptu systems, it is difficult to distinguish conduct peculiarities in course disclosure. Specifically, proposed directing conventions can't avert wormhole assaults. In a wormhole assault, an aggressor brings two handsets into a remote system and associates them with an astounding, low-idleness connect. Steering messages got by one wormhole endpoint are retransmitted at the other endpoint. Assailants can misuse wormholes to manufacture false course data,

specifically drop parcels, and make steering circles to squander the vitality of system.

2. Background

A few secure steering conventions have been proposed for remote specially appointed systems. Papadimitratos and Haas [23] show the SRP convention that secures against non-intriguing foes by handicapping course storing and giving end-to-end validation utilizing a HMAC primitive. SEAD [7] utilizes one-way hash chains to give confirmation to DSDV [21]. Ariadne [8] utilizes a validated communicate strategy [22] to accomplish comparable security objectives on DSR [11]. Marti et al. [16] analyze procedures to minimize the impact of getting out of hand hubs through hub snooping and reporting, yet it is powerless against coercion assaults. ARRIVE [13] proposes probabilistic multi-way directing rather than single way calculation to upgrade the strength of steering. These safe directing conventions are still powerless against wormhole assaults which can be led without having admittance to any cryptographic keys.

Wormhole assaults rely on upon a hub distorting its area. Consequently, area based directing conventions can possibly forestall wormhole assaults [15].

3. Wormhole Attacks

In a wormhole assault, an aggressor advances bundles through a high caliber out-of-band connection and replays those parcels at another area in the system [9, 15]. Figure 1 demonstrates an essential wormhole assault. The assailant replays bundles got by X at hub Y , and the other way around. On the off chance that it would ordinarily take a few bounces for a bundle to cross from an area close X to an area close Y, parcels transmitted close X going through the wormhole will touch base at Y before bundles going through different jumps in the system. The aggressor can make An and B trust they are neighbors by sending steering messages, and after that specifically drop information messages to disturb correspondences amongst An and B.

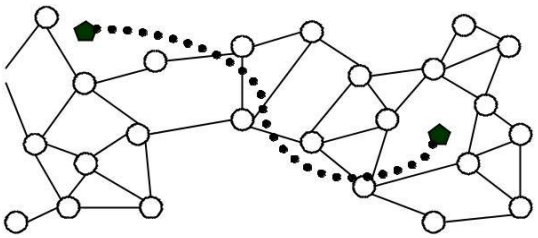


Figure 1. Wormhole attack. The adversary controls nodes *X* and *Y* and connects them through a low-latency link.

A more astute assailant might have the capacity to place wormhole endpoints at

specific areas. Deliberately set wormhole endpoints can upset about all correspondences to or from a specific hub and every other hub in the system. In sensor organize applications, where most interchanges are guided from sensor hubs to a typical base station, wormhole assaults can be especially destroying. On the off chance that the base station is at the side of the system, a wormhole with one endpoint close

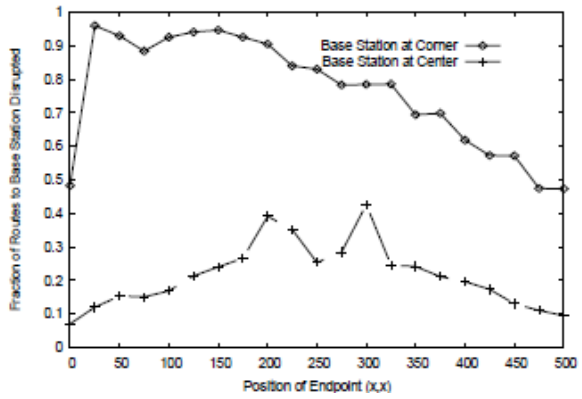


Figure 2. Impact of Wormhole Attack. A strategically placed node can disrupt a substantial fraction of communications.

The position of the second endpoint moves askew over the system (position 250 means the second endpoint is at the focal point of the system; 0 implies it is in the base left corner).the base station and the other endpoint one bounce away will have the capacity to draw in almost all activity from sensor hubs to the base station

4. Directional Antennas

Directional antenna systems are increasingly being recognized as a powerful way for increasing the capacity and connectivity of ad hoc networks [25, 26]. Transmitting in particular directions results in a higher degree of spatial reuse of the shared medium. Further, directional trans-mission uses energy more efficiently. The transmission range of directional antennas is usually larger than that of omnidirectional antennas, which can reduce hops for rout-ing and make originally unconnected devices connected.

When sending messages, a node can work in omni or directional mode. In omni mode signals are received with a gain G^o, while in directional mode with a gain of G^d. Since a node in directional mode can transmit over a longer distance, $G^d > G^o$. The omnidirectional and directional gains can be estimated from [25]. For ex-ample, when the number of zones is 6, and the omni transmission range is 250m, then the directional trans-mission range is 450m [5]. For our simulations, we use the same ratio between omni and directional transmission distances, but scale the ranges to 40m and 72m.

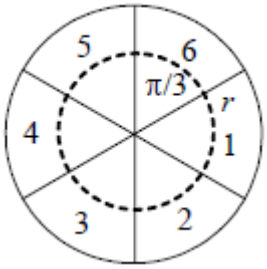


Figure 3. Directional Antenna with 6 zones.

Each zone is a wedge with radius *r* spanning π/3 radians. Zone 1 always faces east. The dashed circle shows the omnidirectional communication radius.

5. Protocols Our way to deal with identifying wormhole assaults relies on upon hubs keeping up precise arrangements of their neighbors. An aggressor can't execute a wormhole assault if the wormhole transmitter is perceived as a false neighbor and its messages are overlooked. One critical property of directional antennas is a hub can get inexact course data in light of got signs. Next we archive our presumptions about the system. At that point, we portray three progressively viable conventions for counteracting wormhole assaults. As directional data is included, assaults turn out to be progressively hard to execute effectively. The principal convention, directional neighbor revelation, does not depend on any participation amongst hubs, and can't counteract numerous wormhole assaults. By sharing data among neighboring hubs, the checked neighbor revelation convention can forestall wormhole assaults where the aggressor controls just two endpoints and the casualty hubs are no less than two jumps inaccessible. At long last, the strict neighbor disclosure convention avoids wormhole assaults notwithstanding when the casualty hubs are adjacent.

5.1 Assumptions

We expect all non-wormhole correspondence channels are bidirectional: if A can hear B, then B can hear A. This is not generally the situation in remote systems, particularly if battery control and physical qualities of antennas fluctuate. With our convention, unidirectional connections can't be built up.

We expect an instrument is accessible to build up secure connections between all sets of hubs and that every single basic message are encoded. A few proficient systems have been proposed for setting up secure connection enters in specially appointed systems [6, 3, 22].

We use the following notation:

A, *B*, *C*...	Legitimate nodes
X, *Y*	Wormhole endpoints
R	Nonce
$E_{KAB}(M)$	Message encrypted by key shared between nodes *A* and *B*
zone	The directional element, which ranges from 1–6 as

^zone	shown in Figure 3 The opposite directional element. For example, if zone=1 then ^zone=4.
zone (A, B)	Zone in which node A hears node B
neighbors (A, zone)	Nodes within one (directional distance) hop in direction zone of node A.

5.2 Directional neighbor discovery

The directional neighbor disclosure convention does not forestall numerous wormhole assaults, but rather it shapes the reason for our different conventions. Quickly after sending, hubs will have no known neighbors. Every hub will haphazardly pick a period and occasionally utilize neighbor revelation convention to upgrade its neighbor set. We call the hub that starts the convention the host.

From Figure 3, one obvious observation is if node *A* is in node *B*'s *zone* direction, then node *B* is in node *A*'s opposite direction ^*zone* (for example, if *zone*=1, ^*zone*=4). We summarize this as:

$A \in \text{neighbors}(B, zone) \Rightarrow B \in \text{neighbors}(A, \hat{}zone)$

This relies on all nodes having the same antenna orientation due to their common magnetic orientation. Because of measurement imprecision, it is possible that the actual zone will be off by one in either direction. For simplicity of this presentation, we assume this observation holds for now. In Section 7, we consider the impact of directional inaccuracies.

The simple directional neighbor discovery protocol works in three steps:

1. $A \rightarrow \text{Region} \quad \text{HELLO} \mid ID_A$

The announcer *A* broadcasts a HELLO message that includes its identity. This is done by transmitting the message in every direction, sequentially sweeping through each antenna in the antenna array.

$N \rightarrow A \quad ID_N \mid E_{\text{KNA}} (ID_A \mid R \mid \text{zone}(N, A))$

All nodes that should hear the HELLO message send their node ID and an encrypted message to the announcer. The message contents are encrypted with a key shared between the announcer and the sender, which the sender can determine based on knowing its own node ID and that of the announcer. The encrypted message contains the announcer's ID, a random challenge nonce, and the zone in which the message was received.

3. $A \rightarrow N\ R$

The announcer decrypts the message and verifies that it contains its node ID. It further verifies that it heard the message in the opposite zone from the zone reported by the neighbor. That is, zone (*A*, *N*) = ^zone (*N*, *A*). If it is correct, it adds the sending neighbor to its neighbor set for zone (*A*, *N*). In the event that the message was not got in the proper zone, it is disregarded. Something else, the broadcaster transmits the unscrambled challenge nonce to the sending neighbor. After accepting the right nonce, the neighbor embeds the broadcaster into its neighbor set. In any case, the neighbor disclosure convention itself is powerless against wormhole assaults. An aggressor with a wormhole can build up a false far off neighbor by sending difficulties and reactions through the wormhole. An advertisement versary with two handsets, one close to the broadcaster and another in an inaccessible territory of the system, can burrow the commentator's HELLO message to the far off zone all through of-band channel. The wormhole hub rebroadcasts the message, and gets challenges from neighboring hubs. It burrows those difficulties through the wormhole, and transmits them to the broadcaster. To the broadcaster, the difficulties seem, by all accounts, to be splendidly real, so the hubs are included and the unscrambled nonces are transmitted. The foe burrows the reactions through the wormhole, and transmits them to the senders. The removed sending hubs will show up as neighbors to the commentator, and the broadcaster will be added to every sending hub's neighbor set.

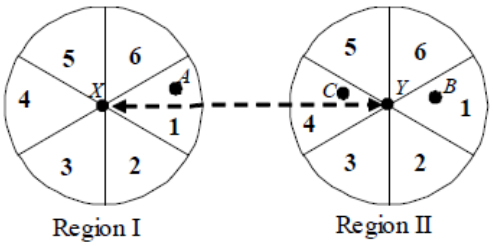


Figure 4. Directional Attack. The adversary establishes a wormhole between *X* and *Y*, and can trick *A* and *C* into accepting each other as neighbors by forwarding messages since they are in opposite zones relative to the respective wormhole endpoints.

5.3 Verified neighbor discovery protocol

In spite of the fact that the basic directional convention does not adequately alleviate the viability of wormhole assaults, it proposes that if hubs coordinate with their neighbors they can avoid wormholes since the aggressor may have the capacity to persuade hubs specifically locales that they are neighbors.

Accept the foe has one handset at every end of the wormhole. As portrayed in the past segment, it can just trap hubs that are in inverse headings from the wormhole endpoints into tolerating each different as neighbors. Hence, nodes in other locations can establish the announcer's legitimacy. We call such nodes *verifiers.*

Consider node *C* in Figure 4. Since *C* receives *A*'s transmissions through *Y* in its zone 1 antenna, all of its neighbors in zone 1 should also be neighbors of *A*. If any of those nodes are in different directions from *Y* (such as node *B* in Figure 4), then the wormhole will not be able to convince them they are neighbors of *A*. Note however, that *C* could be on the other end of the wormhole, as shown in Figure 5. Here, *B* will hear *A* and *C* from the west through the wormhole (zone (*B*, *A*) = zone (*B*, *C*) = 4), and *C* will hear A directly from the east (zone (*A*, *C*) = ^zone(*C*, *A*) = 1) and C will hear B from the west through the wormhole (zone (*C*, *B*) = ^zone (*B*, *C*) = 4). Hence, we need a stricter requirement on verifiers to prevent verifiers from acting through the wormhole.

A valid verifier *V* for the link $A \leftrightarrow B$ must satisfy these properties: zone (*B*, *A*) ≠ zone (*B*, *V*). Node *B* hears *V* in a different zone from node *A*, hence it knows *A* and *V* are in different locations, and both cannot be coming through a single wormhole endpoint zone (*B*, *A*) ≠ zone (*V*, *A*). Node *B* and *V* hear node *A* from different directions. A wormhole can deceive nodes in only one direction. So if both *B* and *V* are directionally consistent with *A* in different directions (zone (*B*, *A*) = ^zone (*A*, *B*) and zone (*V*, *A*) = ^zone (*A*, *V*)), then they know *A* is not being retransmitted through a wormhole.

In Figure 5, *C* cannot act as a verifier since zone (*B*, *A*) = zone (*C*, *A*), failing the first property. Node *D* can act as a verifier, since zone (*B*, *A*) = 4 ≠ zone (*B*, *D*) = 5, and zone (*D*, *A*) = 3 ≠ zone (*B*, *A*) = 4. Note, however, that the wormhole cannot convince *D* and *A* to accept each other as neighbors since zone (*D*, *A*) = 3 ≠ ^zone (*A*, *D*) = 1. Hence, *B* will not be able to verify *A* as a neighbor through *D*.

We modify the original protocol to use verifier nodes to establish legitimate neighbor relationships. The first three steps are the same as in the simple neighbor discovery protocol:

1. $A \rightarrow$ Region HELLO | ID_A

$N \rightarrow AID_N \mid E_{\text{KNA}}\ (ID_A \mid R \mid \text{zone}\ (N, A))$

3. $A \rightarrow N\ R$

These steps authenticate the nodes and their apparent relative positions, but do not establish

that they are communicating without going through a wormhole. Next, the protocol uses a verifier node to confirm the link is not being created through a wormhole:

4. $N \rightarrow$ Region INQUIRY | ID_N | ID_A | zone(N, A) All neighbor nodes that hear the HELLO message broadcast an inquiry in directions except for the received direction and opposite direction. So, if N received the announcement in zone 1, it will send inquiries to find verifiers to zones 2, 3, 5 and 6. The message includes zone (N, A), so prospective verifiers can determine if they satisfy the verification properties by having heard A in a different zone.

5. $V \rightarrow N\ ID_V \mid E_{KNV}$ ($ID_A \mid$ zone (V, N))

Nodes that, receive the inquiry and satisfy the verification properties respond with an encrypted message. This message confirms that the verifier heard the announcement in a different zone from N and has completed steps 1-3 for the protocol to authenticate A and its relative position.

To continue the protocol, N must receive at least one verifier response. If it does, it accepts A as a neighbor, and sends a message to A:

$N \rightarrow A \quad ID_N \mid E_{KAN}$ ($ID_A \mid$ ACCEPT)

After receiving the acceptance messages, the announcer adds N to its neighbor set.

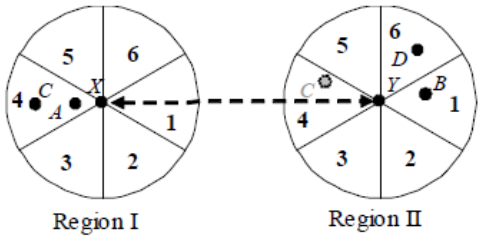


Figure 5. Verifiers. Node *C* cannot act as a verifier for the link *A*↔*B* since the wormhole attacker could make a node on the other end of the wormhole appear. Node *D* could act as a verifier, since it satisfies the verifier properties.

5.4 Strict neighbor discovery protocol

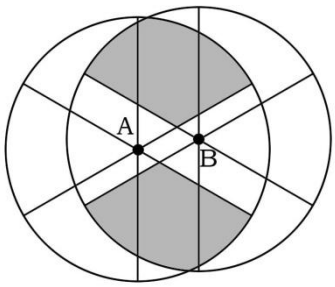


Figure 6 shows the verifier region of two neighbor nodes. If there is a node in the shaded region, it can act as a verifier for *A* and *B*. However, the verifier region may still exist when two nodes are slightly out of radio range, and a smart adversary can use this to make them to be neighbors.

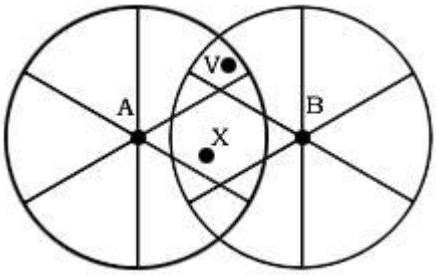


Figure 7 depicts the Worawannotai attack in which the adversary convinces two nearby (but not neighboring) nodes they are neighbors. Node *B* is located just beyond the transmission range of node *A*.

There will be two areas that could have valid verifier for this protocol. If there is a valid verifier in those areas, the attacker can just put one node in between *A* and *B* (node *X* in Figure 7) and use it to listen to and retransmit messages between *A* and *B*. Nodes *A* and *B* will mistakenly confirm they are neighbors using verifier *V*, but the attacker will have control over all messages between *A* and *B*.

The Worawannotai attack will succeed only if the victim nodes (*A* and *B* in the figure) are unable to communicate directly, but are close enough to have a verifier that can hear both *A* and *B*. Assuming perfect transmission distances, this means *A* and *B* must be more than *r* distance apart, but less than

$$2r \cos\pi / 6 = r\sqrt{3}$$

after which the size of the false verification region is zero. If *A* and *B* are aligned horizontally, the size of the areas that could contain false verifiers is

$$4\int_{\frac{r}{2}}^{\frac{r+a}{2}} \sqrt{1-x^2} - \frac{\sqrt{3}}{2}\, dx$$

where $r + a$ is the distance between *A* and *B*. The maximum area is slightly less than 15% of the transmission area in the worst case where *A* and *B* are just over *r* distance apart (*a* is 0), and decreases substantially as the distance increases.

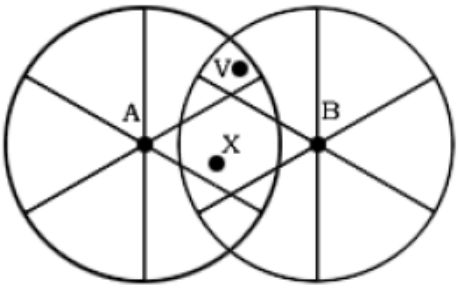


Figure 7. Worawannotai attack.

To prevent the Worawannotai attack, we need to place additional constraints on verifiers. The strict neighbor discovery protocol exchanges the same messages as verified neighbor discovery protocol but has stricter requirements on verifiers. In strict protocol, a valid verifier *V* for the link $A \leftrightarrow B$ must satisfy these three properties:

zone(B, A) ≠ zone (B, V).

zone(B, A) ≠ zone (V, A).

zone(B, V) cannot be both adjacent to zone(B, A) and adjacent to zone(V, A).

The initial two conditions are the same as past convention, and they ensure that the foe can't replay the affirmation message from verifiers. The third condition guarantees that the verifier district is void when two hubs are out of radio range, so the foe can't utilize this to lead Worawannotai assault.

Figure 8 demonstrates the verifier area of the strict convention. Contrasted and Figure 6, we can see that the district amongst An and B is no longer contains verifiers. We next demonstrate that the shaded territories can't contain any verifiers if An and B are more distant than r separate separated, and henceforth, the Worawannotai assault will fail.

We consider the region above and left of A; the proof for

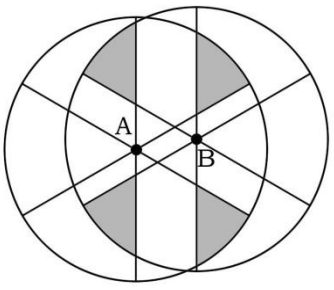


Figure 8. Strict Verifier Region. The shaded area is the verifier region of node A and B in strict neighbor discovery protocolall other regions is equivalent. All potential verifiers *V* in that region have zone (*V*, *A*) = 2 and zone (*V*, *B*) = 2.

Let x_N denote the x coordinate of node N, d_{NM} the actual distance between nodes N and M, and θ_{NM} the angle between nodes N and M relative to the horizontal axis.

For a verifier V in the above left region, we have:

$x_V = x_A + d_{AV} \cos \theta_{AV}\, x_V = x_B + d_{BV} \cos \theta_{BV}\, x_B = x_A + d_{AB} \cos \theta_{AB}$

Because zone(V, A) = 2 and zone (V, B) = 2, we know θ_{AV} and θ_{BV} are between $\pi/2$ and $5\pi/6$. Hence, the minimum value of cos θ_{AV} is 0 for $\pi/2$. So, we know $x_V \leq x_A$ and $x_V \leq x_B$. This makes sense since V must be to the left of both A and B. Substituting the expansion of x_B from the third equation into the second equation, we have,

$x_V = x_A + d_{AB} \cos \theta_{AB} + d_{BV} \cos \theta_{BV}$

Since zone (A, B) = 1, θ_{AB} is between $-\pi/6$ and $\pi/6$. Minimizing the values of the cosines, we have

$x_V \geq x_A + d_{AB} \cos \pi/6 + d_{BV} \cos 5\pi/6.$

The Worawannotai attack is possible only if $d_{AB} > r$ and $d_{BV} \leq r$. So, this implies $x_V > x_A$ which contradicts $x_V \leq x_A$ and proves that no

false verifier could exist. Similarly, we can prove that all other three shaded regions are also empty if *A* and *B* are further than one hop apart.

5.5 Discussion

The strict neighbor revelation convention anticipates wormhole assaults when the enemy has just two endpoints. An aggressor with numerous endpoints could specifically forward parcels through various endpoints to set up false neighbors. In the extraordinary, an assailant who can encompass a specific target hub with wormhole endpoints can make messages touch base in any zone by transmitting them through an alternate endpoint. Our resistance does not keep numerous endpoint assaults, despite the fact that it ought to be noticed that the assets important to do such an assault are generous.

The overhead connected with our convention is insignificant, the primary cost is the potential loss of legitimate connections (talked about in the following segment). For pairwise key circulation, the run of the mill procedure to safely find one connection (without imperviousness to wormhole assaults) includes hub declaration, test and reaction (3 messages). Our convention includes extra messages for request, check and acceptance.from the third condition into the second condition, we have,

$$x_V = x_A + d_{AB} \cos \theta_{AB} + d_{BV} \cos \theta_{BV}$$

Since zone $(A, B) = 1$, θ_{AB} is between $-\pi/6$ and $\pi/6$. Minimizing the values of the cosines, we have

$$x_V \geq x_A + d_{AB} \cos \pi/6 + d_{BV} \cos 5\pi/6.$$

The Worawannotai attack is possible only if $d_{AB} > r$ and $d_{BV} \leq r$. So, this implies $x_V > x_A$ which contradicts $x_V \leq x_A$ and proves that no false verifier could exist. Similarly, we can prove that all other three shaded regions are also empty if *A* and *B* are further than one hop apart.

5.5 Discussion

The strict neighbor disclosure convention averts wormhole assaults when the foe has just two endpoints. An assailant with numerous endpoints could specifically forward bundles through various endpoints to set up false neighbors. In the outrageous, an assailant who can encompass a specific target hub with wormhole endpoints can make messages touch base in any zone by transmitting them through an alternate endpoint. Our guard does not keep various endpoint assaults, in spite of the fact that it ought to be noticed that the assets

important to complete such an assault are significant.

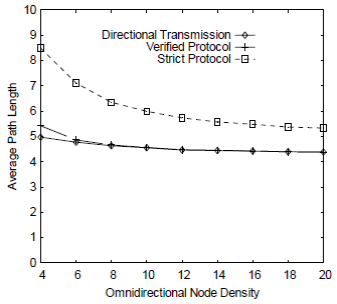
The overhead connected with our convention is negligible, the fundamental cost is the potential loss of substantial connections (talked about in the following segment). For pairwise key dissemination, the run of the mill procedure to safely find one connection (without imperviousness to wormhole assaults) includes hub declaration, test and reaction (3 messages). Our convention includes extra messages for request, check and acknowledgment.

One conceivable, however improbable, assault is to utilize magnets to endeavor to perplex hubs. An aggressor could utilize a magnet to control the introduction of a hub to make it get messages in the proper zone. This would require tight coordination between the wormhole retransmitting parcels and the magnet controller. For the case in Figure 4, a venturesome aggressor could retransmit hub A's declaration through the wormhole. Before transmitting B's reaction, the aggressor would utilize a magnet to perplex A one half revolution so its east zone is currently confronting west. Consequently, A would acknowledge B's reaction as originating from the other way (despite the fact that it really originated from a similar course). Take note of that the assailant would need to reorient An effectively before it conveys the following message. By and by, it is far-fetched that a magnet assault should be possible effectively as a result of the physical nosiness and timing accuracy required. As a rule, it would be simpler for an aggressor to set up various endpoints.

6. Analysis

Our conventions have low overhead, however may impact the general execution of the system by keeping true blue connections from being built up. In this segment we break down the effect of our conventions on hub availability and steering execution. In both the confirmed convention and the strict convention, it is conceivable that in step 3, there are no potential verifier hubs. Without a verifier hub, N can't recognize honest to goodness neighbors from neighbors through a wormhole. Hubs close to the border of the system are particularly inclined idealistic system will proceed with the convention and acknowledge the commentator without check, while a moderate methodology will dismiss the broadcaster and stop the convention.

to having no verifier hubs. For this situation, an



The primary decision licenses fruitful wormhole assaults while the second decision may keep some honest to goodness hubs from joining the system. Since the harm an effective wormhole assault can bring about is significant, we embrace the more traditionalist decision: a hub will just acknowledge another hub as a neighbor on the off chance that it can be confirmed by no less than one verifier.

7. Directional Errors

As such, we have accepted hubs dependably hear each other in specifically inverse bearings (e.g., if hub A hears hub B in zone 1, hub B hears hub An in zone 4). In a commonplace sending, this is frequently not the situation. On the off chance that hubs are close to the move point between two zones, little contrasts in hub introduction, reception apparatus arrangement and pick up, and transmission inconsistencies will prompt to honest to goodness hubs seeming, by all accounts, to be in the wrong zone. As result, a few connections between real neighbors will be lost.

Figure 11. Impact on routing path length.

8. Conclusion

Wormhole assaults are an intense assault that can be led without requiring any cryptographic breaks. An aggressor who directs an effective wormhole assault is in a position to upset steering, refuse assistance to expansive sections of a system, and utilize particular sending to mess with system applications. Directional antennas offer a promising way to deal with counteracting wormhole assaults. They are less costly than numerous systems proposed for restriction, and offer different focal points notwithstanding security including more proficient utilization of vitality and better spatial utilization of data transfer capacity. The conventions we propose lessen the danger of wormhole assaults with negligible loss of system availability. Given the absence of accessibility of other appropriate barriers and the potential harm a fruitful wormhole assault can incur, this tradeoff is alluring for some applications.

References

[1] N. Bulusu, J. Heidemann and D. Estrin. *GPS-less Low Cost Outdoor Localization*

for Very Small Devices. IEEE Personal Communications Magazine, October 2000.

[2] S. Bandyopadhyay, K. Hausike, S. Horisawa and S. Tawara.

An Adaptive MAC and Directional Routing Protocol for Ad Hoc Wireless Networks Using ESPAR Anenna.

ACM/SIGMOBILE MobiHoc October 2001.

[3] H. Chan, A. Perrig and D. Song. *Random Key Predistribution Schemes for Sensor Networks.* IEEE Symposium on Security and Privacy 2003.

[4] R. Choudhury, X. Yang, R. Ramanathan and N. Vaidya.

Using Directional Antennas for Medium Access Control for Ad Hoc Network. ACM MobiCom 2002, September 2002.

[5] R. Choudhury and N. Vaidya. *Ad Hoc Routing Using Directional Antennas*. University of Illinois, Coordinated Science Laboratory, Technical Report, August 2002.

[6] L. Eschenauer and V. Gligor. *A Key-Management Scheme for Distributed Sensor Networks*. ACM Conference on Computer and Communication Security, November 2002.

[7] Y. Hu, D. Johnson, and A. Perrig. *SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks.*

IEEE Workshop on Mobile Computing Systems and Applications, June 2002.

[8] Y. Hu, A. Perrig and D. Johnson. *Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks*. ACM MobiCom 2002, September 2002.

[9] Y. Hu, A. Perrig, and D. Johnson. *Packet Leashes: A Defense against Wormhole Attacks in Wireless Ad Hoc Networks*. INFOCOM 2003, April 2003.

[10] T. He, C. Huang, B. Blum, J. Stankovic and T. Abdelzaher.

Range-Free Localization Schemes for Large Scale Sensor Networks. ACM MobiCom 2003, September 2003.

[11] D. Johnson, D. Maltz, and J. Broch. *The Dynamic Source Routing Protocol for Multihop Wireless Ad Hoc Networks.*

In Ad Hoc Networking, C. Perkins, Ed. Addison-Wesley, 2001.

[12] T. Korakis, G. Jakllari and L. Tassiulas. *A MAC protocol for full exploitation of Directional Antennas in Ad-hoc Wireless Networks.* MobiHoc 2003.

[13] C. Karlof, Y. Li, J. Polastre. *ARREVE: Algorithm for Robust Routing in Volatile Environments.* Technical Report UCB//CSD-03-1233, March 2003.

[14] Y. Ko, V. Shankarkumar and N. H. Vaidya. *Medium access control protocols using directional antennas in ad hoc networks*. IEEE INFOCOM, 2000.

[15] C. Karlof and D. Wagner. *Secure Routing in Sensor Networks: Attacks and Countermeasures*. First IEEE International Workshop on Sensor Network Protocols and Applications, May, 2003.

[16] S. Marti, T. J. Giuli, K. Lai, and M. Baker. *Mitigating routing misbehavior in mobile ad hoc networks.* ACM/IEEE International Conference on Mobile Computing and Networking, 2000.

[17] A. Nasipuri, J. Mandava, H. Manchala and R. E. Hiromoto.

On Demand Routing Using Directional Antennas in Mobile Ad Hoc Networks. IEEE Wireless Communications and Networking Conference (WCNC), September 2000.

[18] D. Niculescu and B. Nath. *Ad Hoc Positioning System (APS) using AoA.* INFOCOM 2003.

[19] R. Nagpal, H. Shrobe and J. Bachrach. *Organizing a Global Coordinate System from Local Information on an Ad Hoc Sensor Network*. 2nd International Workshop on Information Processing in Sensor Networks (IPSN '03), April, 2003.

[20] A. Nasipuri, S. Ye, J. You, R.E. Hiromoto. *A MAC protocol for mobile ad-hoc networks using directional antennas.*

IEEE Wireless Communications and Networking Conference, September 2000.