

# New Variants of Wormhole Attacks for Sensor Networks

Waqqas Sharif

Department of Computer Science and Software Engineering  
The University of Melbourne  
Melbourne, Australia  
sharifw@unimelb.edu.au

Christopher Leckie

NICTA Victoria Research Laboratory  
Department of Computer Science and Software Engineering  
The University of Melbourne  
Melbourne, Australia  
caleckie@csse.unimelb.edu.au

**Abstract**— In multi-hop mobile wireless systems such as sensor networks, nodes have limited energy, computation capability and transmission power. In such systems there is a need for cooperation between nodes to route each other's packets. This exposes these nodes to wide range of security attacks. A particularly disruptive form of attack is the wormhole attack, where an adversary records packets received in one part of the network and replays them in different parts of the network. Wormhole attacks can cause severe damage to the route discovery mechanism used in many routing protocols. In this paper we propose three new variants of the wormhole attack, and explain how these new variants of wormhole attack deplete energy and disrupt service in the network.

**Keywords:** *Wireless Sensor Networks; Security; Secure routing*

## I. INTRODUCTION

Wireless sensor networks are autonomous systems consisting of tiny sensors that are equipped with integrated sensing, general purpose computing and limited-range transceiving capabilities. Due to their ad-hoc deployment, sensor nodes require mutual coordination and cooperation to route information within the network. Each node acts as a router for packets, which means that each intermediate node has full access to the packets flowing through it. These factors make sensor networks potentially vulnerable to several different types of malicious attacks.

A particularly devastating security attack known as a *wormhole* has been discussed in the context of ad-hoc networks [1, 2] where a malicious node records packets in one location, and with the help of another colluding node replays the packet in a distant part of the network. The colluding nodes can use communication techniques such as an out-of-band channel (a point-to-point link) or high power transmission (using directional antennas) to tunnel packets. This tunneling enables the tunneled packet to arrive with fewer hops or lower delay than if the packet traversed a normal path. The arrival of packets with low delay or hop count attracts nearby traffic towards the malicious node, thus affecting routing. Wormhole attacks are particularly damaging for many ad hoc network protocols such as AODV [3] and DSR [4] in which the node that hears a packet transmission from some other node considers that node as its neighbor. Note that wormhole attack is still possible even if the adversary does not have access to

the contents of the packet payload, i.e., the packet contents are encrypted. Wormhole attacks can be hard to detect, as they do not inject abnormal volumes of traffic into the network.

Wormhole attacks have been discussed in the context of how they affect route discovery [2], using at least two malicious nodes to launch an attack. However, there has been little analysis of how these attacks effect the lifetime of sensor networks. In this paper we highlight that how an attacker can significantly reduce the network lifetime by launching energy depletion attacks. Furthermore, the attacks that we introduce only require a single malicious node to launch the attack, which makes them easier for an adversary to implement. An attacker does this by tunneling route request and route reply messages in the network. In particular, we demonstrate how an attacker can indirectly make innocent nodes appear as the source of the attack. We also investigate the effectiveness of increasing the number of base stations in the network as a means of reducing the impact of these attacks.

Section II discusses relevant previous work on ad-hoc network attacks. In Section III we describe our new proposed variants of wormhole attacks. We then analyze these variants in Section IV. Our simulation environment and the results of our simulation are presented in Sections V and VI respectively. Section VII describes known defenses and our proposed solution to overcome wormhole attack.

## II. PREVIOUS WORK

### A. Denial of Service based Wormhole Attack

Wormhole attacks can be used as form of denial of service (DoS) attack [2]. The aim of this attack is to prevent legitimate Route Request (RREQ) messages from reaching their destination. If a node needs to discover route to a given destination, it broadcasts a RREQ packet. A high powered ("laptop-class") attacker can exploit this by tunneling each RREQ packet directly to a partner malicious node near the destination node of the RREQ. The partner node then broadcasts the RREQ to all its neighbors. When the destination node's neighbors hear this packet, they will follow the normal operation of the routing protocol by re-broadcasting that copy of the RREQ, and dropping all subsequent RREQ packets that are received for the same route discovery. This dropping of RREQ packets is an essential part of the AODV protocol to

avoid redundant broadcasts. This attack thus prevents a legitimate RREQ from reaching the destination through a legitimate path. The request will reach the destination, but the intermediate nodes will not have the reverse route to the source of the RREQ, so it cannot forward the Route Reply (RREP).

### B. Indirect Sinkhole Attack (ISA)

Another malicious use of wormholes is in an indirect sinkhole attack [5], which is used to lure traffic to a malicious node so that it can selectively forward the packets. To launch this attack an attacker needs two high powered (“laptop-class”) malicious nodes. An attacker puts the first malicious node near the destination node and the second malicious node near the source node. When a RREQ sent by the source node reaches the destination, the destination sends a RREP packet towards the source. The first malicious node hears this RREP packet and tunnels it directly to its partner node. Due to tunneling the RREP contains fewer hops than a legitimate RREP. The second malicious node then forwards the tunneled RREP towards the source node. The source node and all nearby nodes then use second malicious node as their next hop towards the destination. Consequently, this attack puts the attacker in a very strong position to selectively forward packets.

## III. OUR CONTRIBUTION – NEW WORMHOLE ATTACKS

We have identified three new variants of the wormhole attack, which create a Denial of Service (DoS), and reduce the lifetime and throughput of the network. The attacker in these variants uses high power transmission in order to launch the attacks. These variants are examples of outsider attacks, where an adversary injects a single malicious node into the network.

We have proposed three new variants of the wormhole attack.

1. Energy Depleting Wormhole Attack (EDWA)
2. Indirect Black hole Attack (IBA)
3. Targeted Energy Depleting Wormhole Attack (TEDWA)

TABLE I. COMPARISON OF DIFFERENT VARIANTS OF WORMHOLE ATTACK

Attack	No. of malicious nodes	Motives	Tunneled packet type	Impact
DoS	2	DoS	RREQ	Medium
ISA	2	DoS	RREP	Medium
EDWA	1	DoS, Deplete Energy	RREQ	Low
IBA	1	DoS, Deplete Energy	RREP	Medium
TEDWA	1	DoS, Deplete Energy	RREP	Medium

### A. Energy Depleting Wormhole Attack (EDWA)

The motive of this attack is to reduce network lifetime. An attacker achieves this by placing a single malicious node  $A$  having laptop class capability near the source  $S$  of the RREQ packet. The attacker does not require another malicious node to be present in the network as the recipient of the tunneled

RREQ message can be any legitimate node near the destination. The attacker exploits the fact that each node only processes the first RREQ instance it receives, and ignores later instances of the same RREQ. If a node  $S$  wants the route to the destination  $D$ , it first broadcasts a RREQ to all its neighbors. The malicious node  $A$  will hear this broadcast and tunnel the RREQ to an ordinary node  $V$  near the destination using a directional antenna or high-powered transmission. When the ordinary node hears this RREQ, it further broadcasts the RREQ to its neighbors. When the RREQ reaches the destination  $D$ , it sends a RREP packet that is destined for the original source node  $S$ . When the ordinary node  $V$  receives the RREP, it does not have the reverse route to the source  $S$ , so it discards that RREP packet. Nodes near the destination will drop the legitimate RREQ as they already have seen this packet as a result of the tunneling. Consequently, the legitimate RREQ does not reach the destination.

As the first routing attempt was unsuccessful, the source node  $S$  will try again after a waiting period. The malicious node  $A$  will hear this new RREQ and again tries to tunnel the RREQ to the ordinary node  $V$ . This time the ordinary node  $V$  after receiving the tunneled RREQ will not broadcast the tunneled RREQ packet as now it has the route to the destination. Consequently,  $V$  tries to send a RREP to the source node. The ordinary node  $V$  will fail again as it does not have the reverse route to the source node. However this time the legitimate RREQ will reach the destination  $D$  traversing the legitimate path. Now all the intermediate nodes between the source and destination have the reverse route to the source node, so the RREP sent by the destination would reach the source node.

As a result of the tunneled RREQ, the nodes in the network have to broadcast the RREQ at least twice, in order to obtain the route to the destination. Broadcasting is a very energy intensive activity as it requires every node in the network to receive and rebroadcast the packet. So if every route request takes at least two attempts to be successful, then it clearly reduces the network lifetime. This attack can also result in DoS, if there is no other path to the destination for the RREQ.

### B. Indirect Black Hole Attack (IBA)

The indirect black hole attack is used to lure traffic into the vicinity of a specified node in order to create a DoS attack and deplete the energy of that node. The attacker uses a powerful transmitter or directional antenna to tunnel RREP messages. An attacker puts the malicious node  $A$  near the destination node  $D$ . When a RREQ reaches destination  $D$  it sends a RREP packet towards the source node  $S$ . The malicious node  $A$  will then hear this RREP packet, and tunnels it directly to the victim node  $V$ , which is near the source node. Due to tunneling, the RREP contains fewer hops. The victim node  $V$  then forwards the tunneled RREP towards the source node. The source node and all nearby nodes then mark the victim node as their next hop towards the destination. This creates a black hole, as the victim node  $V$  has an incomplete route towards the destination and has to drop all packets that are sent to it by nearby nodes to forward to the destination node. When the legitimate RREP approaches the source node, it will be dropped by either the source node or by intermediate nodes as it contains a higher hop count to the destination.

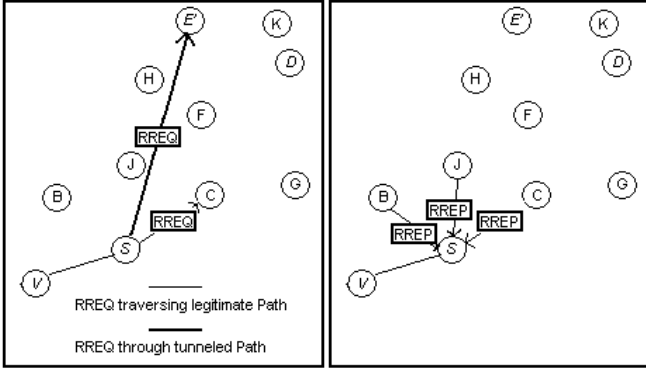


Figure 1. Working of EDWA and TEDWA attack

The choice of ordinary node  $V$  can be changed by the attacker over time, depending on the location of the source node that is requesting a route to the destination.

### C. Targeted Energy Depleting Wormhole Attack (TEDWA)

This variant of the wormhole attack is launched by using a single malicious node that has a powerful transmitter near the destination node. The motive of this attack is to deplete the energy of a particular node in the network. An attacker  $A$  does this by overhearing a RREP destined to a node  $S$ , and then tunnels this RREP to different parts of the network. In normal circumstances the RREP is only unicast to the source node through a single path. The attacker exploits the fact that all nodes have a reverse route to the source node, which has initiated the route discovery. Due to tunneling of the RREP to different parts of the network, the source node receives multiple RREP packets from different nodes in the network rather than a single RREP. In some cases if the tunneled RREP reaches the source node earlier than the RREP through the legitimate path then it can result in a DoS. This attack also affects those parts of the network where the attacker has tunneled the RREP, creating multiple sink holes.

## IV. ANALYSIS OF ATTACKS

In this section we analyze the conditions under which these new variants of the wormhole attack are successful. All these variants exploit the route race condition, such that applicability depends on the number of hops between the source and the destination.

The EDWA attack is the easiest to launch as RREQ messages are broadcast to the whole network, and an attacker can hear one of these RREQ messages. However, this attack has limited effect since the tunneled RREQ message must reach the destination before the RREQ message that traverses the legitimate path.

For RREQ based attacks the following condition should be met:

$$H_{mv} + H_{vd} < H_{sd} \quad (1)$$

Note that  $H_{mv} = 1$  as it is a single hop, so that

$$1 + H_{vd} < H_{sd} \quad (2)$$

where

$H_{mv}$  is the number of hops between the malicious node and the node that receives the tunneled RREQ packet;

$H_{vd}$  is the number of hops between the node that receives the tunneled RREQ packet and the destination node;

$H_{sd}$  is the number of hops between the source and the destination (or a node having a route to the destination).

Only if condition (2) is fulfilled will the tunneled packet reach the destination node earlier than the packet through the legitimate path.

Unlike RREQ messages, RREP based attacks such as IBA and TEDWA send RREP messages using unicast over a single path. This means that the malicious node needs to hear this RREP message in order to launch the attack. The distance between the malicious node and the source node does not matter, as the source node will still accept this RREP as it has traversed fewer hops.

## V. EVALUATION OF ATTACK IMPACT

### A. Simulation Setup

To evaluate the effectiveness of the proposed attacks, we simulated the AODV protocol in NS-2 [6] with the NRL sensor network extension [7]. The goal of our evaluation is to test the effectiveness of our proposed wormhole attack variations under normal and attack conditions. As our proposed attacks have different effects and operate under different scenarios, we simulated each proposed attack under appropriate conditions. The simulation parameters that are same for each variation of wormhole attack are listed in Table II.

### B. Metrics

We have used the following metrics to evaluate the effects of the proposed attacks.

- **Route Request Sent:** This metric counts how many RREQ messages were sent during the simulation time. Fewer message transmissions will prolong the lifetime of the network.
- **Route Reply Received:** This metric counts the number of RREP messages received by the source node of the RREQ. In terms of energy, it is better to have fewer RREP messages received during route discovery.
- **Average Lifetime:** This metric measures the average lifetime of the network, which is calculated by taking the average remaining battery life of all nodes in the network.
- **Network Throughput.** This metric measures the network throughput for sensor nodes that generate data packets to be sent to the base station.
- **Data Packets Received By Base Station.** This metric counts the number of data packets that are received by the base station.

TABLE II. SIMULATION PARAMETERS

<b>Examined Protocol</b>	AODV
<b>Simulator</b>	NS-2
<b>Simulation time</b>	60 Seconds
<b>Simulation area</b>	1000m x 1000m
<b>Number of sensor nodes</b>	208
<b>Number of phenomena nodes</b>	1
<b>Number of base stations</b>	1
<b>Number of malicious nodes</b>	1
<b>Transmission range</b>	250m
<b>Movement model</b>	Pre-defined
<b>Traffic type</b>	CBR(UDP)
<b>Initial energy</b>	5J
<b>RxPower</b>	1.75mW
<b>TxPower</b>	1.75mW
<b>SensePower</b>	1.75mW
<b>IdlePower</b>	1.75 $\mu$ W

## VI. RESULTS AND ANALYSIS

The simulation results in Table III show that more nodes died within the simulation time under the EDWA attack than under normal conditions. Due to the tunneling of RREQ messages, not every route request is fulfilled at the first attempt. Some source nodes have to broadcast RREQ messages more than once depending on their distance from the destination node and the node chosen by attacker to tunnel the RREQ message. Broadcasting more than once for a route request depletes the energy of the nodes, thus leaving more dead nodes under the EDWA attack.

Table III show that the average energy of the network is less under the EDWA attack than under normal conditions, as a RREQ requires every node in the network to receive and broadcast the RREQ message. This reduces the lifetime of the entire network. From Table III we can see that the EDWA attack minimizes the network lifetime by  $\sim$ 20%, whereas the network throughput analysis provided in Table IV shows that

TABLE III. NETWORK LIFETIME ANALYSIS FOR EDWA AND TEDWA ATTACKS

Condition	Time when victim node died (sec)	Total number of nodes died	Avg. energy remaining
Normal	-	41	1.30 J
EDWA	-	55	1.05J
Normal	42.7	-	1.61J
TEDWA	30.8	-	1.59J

TABLE IV. NETWORK THROUGHPUT ANALYSIS

Condition	RREQ sent	RREP received	Throughput of data packets sent, compared to normal	Success rate of packet received by BS
Normal	75	178	-	84.7%
EDWA	105	180	96.7%	73.4%
Normal	59	113	-	77.5%
IBA	40	90	100%	22.4%
Normal	48	71	-	76.6%
TEDWA	36	101	76.6%	0%

the EDWA attack reduces network throughput by 3.3%. The success rate of data packets received by the base station dropped to  $\sim$ 73.9% from 84.7% under normal conditions.

As discussed above, the motive of the IBA attack is to create a DoS in the network. Due to tunneling of the RREP messages, the node selected by attacker becomes a black hole in the network. All the packets sent to this node will be discarded, as this node does not have a route to the base station. Analysis of the IBA attack can be seen from Table IV. Under normal conditions the base station receives more packets, since under the IBA attack most of the packets are sent towards the black hole created by the attacker. The success rate of the data packets that have reached the base station under normal conditions was reduced significantly from 77% to 22%.

In the TEDWA attack, an attacker targets a specific node to deplete its energy by tunneling a RREP message to different nodes in the network. Due to tunneling of the RREP message, the source node receives multiple RREP messages instead of a single RREP message. The lifetime of the source node is longer under normal circumstances when it receives a single RREP message. Under a TEDWA attack the source dies earlier due to receiving multiple RREP messages that consume more energy. The amount of energy depleted in the victim depends on how many nodes have been chosen by the attacker to tunnel the RREP. From Table IV it can be observed that under the TEDWA attack, the victim node received 30% more RREP packets than under normal operation. Similarly from Figure 2 we can see that under the TEDWA attack the lifetime of victim node was reduced by 28%.

## VII. DEFENSES

Table V shows some of the defense schemes that have been proposed for wormhole attacks. Each approach relies on different assumptions and in some cases requires specialized hardware to detect and counter the wormhole attack. Packet leash [3] overcomes wormhole attacks by restricting the maximum distance of transmission, using either tight time synchronization (temporal leashes) or location information (geographic leashes). An alternative approach was introduced by [5], which relies on a neighborhood list. Each node only sends/receives packets from those nodes that are in its neighborhood list. RF watermarking [8] modulates the radio waveform in a specific pattern, and any change in the pattern is

TABLE V. COMPARISON OF DIFFERENT DEFENSE SCHEMES USED AGAINST WORMHOLE ATTACKS

Defense Name	Detects	Special Requirements
Packet Leashes [3]	Outsider, Insider	GPS and synchronized clocks
LITEWORP [5]	Outsider, Insider	None
RF Watermarking [8]	Outsider	None
Directional Antenna [9]	Outsider, Insider	Directional Antennas
SECTOR [10]	Outsider	Special transceiver module
MDS-VOW [11]	Outsider	None

used to trigger the detection. In [9], the concept of using directional antennas was introduced, where each node shares a secret key with every other node and maintains accurate sets of its neighbors. SECTOR [10] uses a distance-bounding algorithm to determine the distance between two communicating nodes. MDS-VOW [11] uses multi-dimensional scaling to reconstruct the network and detects the attack by visualizing the anomaly introduced by the wormhole, based on the distance of neighbors to a central server.

To overcome the effects of these attacks we have taken a different but relatively simple approach of having multiple base stations in the network. Using multiple base stations reduces the effects of DoS by providing alternative paths that bypass the effects of the malicious node. Our simulation results in Figure 3 shows that as we begin to increase the number of base stations then the throughput of data packets received by each base station increases. However, when the number of base stations reaches a certain threshold the throughput of the data packets received by base station starts to decrease. This is due to the congestion caused by the transmission of extra routing packets to/from the additional base stations. Thus, there are diminishing returns for increasing the number of base stations.

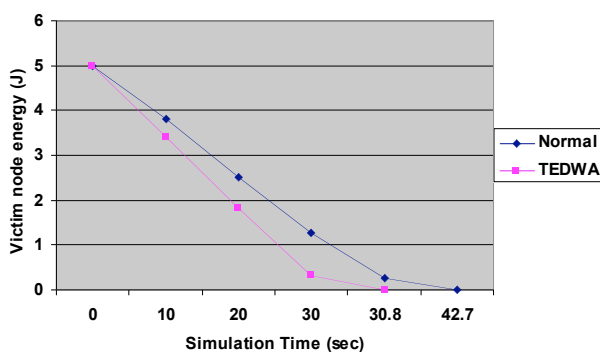


Figure 2. Comparison of victim node energy under normal and TEDWA attack

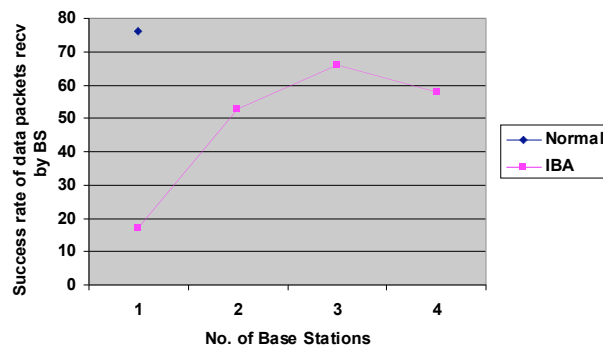


Figure 3. Comparison of data packets received by the base stations under IBA attack with increasing number of base stations

## VIII. CONCLUSION

Security is a vital problem in wireless sensor networks, as they are often deployed in insecure environments. In this paper we have identified new variants of the wormhole attack. The attacks identified in this paper only require a single malicious node, thus making it easier for an adversary to launch an attack. These new variants of wormhole attack have serious consequences on the network, as they cause DoS, reduction of network throughput and reduction in network lifetime. In particular, the IBA attack can cause an innocent victim node to appear as a black hole, which can confuse defenders as to the true source of the attack.

## REFERENCES

- [1] C. Karlof and D. Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures." In Proceedings of the First IEEE International Workshop on Sensor Network Protocols and Applications, May 2003, pp. 113-127.
- [2] Y. Hu, A. Perrig, D. Johnson, Packet leashes: A defense against wormhole attacks in wireless ad hoc networks, in: Proceedings of INFOCOM 2003, 2003
- [3] C. Perkins and E. Royer, "Ad-hoc On Demand Distance Vector Routing." In Proceedings of the Workshop on Mobile Computing Systems and Applications (WMCSA '99), February 1999, pp 90-100.
- [4] D. B. Johnson, D. A. Maltz, and Y. Hu, "The dynamic source routing protocol for mobile ad hoc networks (dsr)," IETF MANET, Internet Draft (work in progress), 2003.
- [5] Issa Khalil, Saurabh Bagchi, Ness B. Shroff: LITEWORP: A Lightweight Countermeasure for the Wormhole Attack in Multihop Wireless Networks. DSN 2005: 612-621
- [6] NS, "The network simulator," <http://www.isi.edu/nsnam/ns/>, 1989.
- [7] I. Downard, "Simulating sensor networks in ns-2," Naval Research Laboratory, "NRL Formal Report 5522-04-10, 2004.
- [8] Defense Advanced Research Projects Agency. Frequently Asked Questions v4 for BAA 01-01, FCS Communications Technology. Washington, DC., October 2000.
- [9] L. Hu and D. Evans, "Using Directional Antennas to Prevent Wormhole attacks," in Network and Distributed System Security Symposium, 2004.
- [10] S. Capkun, L. Buttyan, and J. Hubaux, "Sector:secure tracking of node encounters in multi-hop wireless networks," Proceedings of the ACM Workshop on Security of Ad Hoc and Sensor Networks, 2003.
- [11] W. Wang and B. Bhargava, "Visualization of wormholes in sensor networks," Proceedings of the ACM Workshop on Wireless Security (WiSe), pp. 51-60, 2004.