A WIRELESS PROTOCOL FOR PRODUCTION AGAINST WORMHOLE ATTACKS IN NETWORK CODING SYSTEMS

M. Leenus* & K. Ramamoorthy**

* PG Scholar, Department of Master of Computer Applications, Dhanalakshmi Srinivasan Engineering College, Perambalur, Tamilnadu

** Assistant Professor, Department of Master of Computer Applications, Dhanalakshmi Srinivasan Engineering College, Perambalur, Tamilnadu

Abstract:

Wireless network is now an interesting area of research. As an increasing number of people are going wireless, reducing the culpability of wireless networks is becoming a top priority. The wormhole attack is very powerful and preventing the attack has proven to be very difficult. A strategic placement of the wormhole can result in a significant breakdown in communication across a wireless network. This project designed and developed a new protocol that prevents wormhole attacks on wireless networks. It is only based on the local information that can be obtained from regular network coding protocols, and thus does not introduce any overhead by extra test messages. Increase the system performance of wireless Network, network coding is shown to be effective approach and it is totally different from traditional network. If wormholes attacks are begin in routing, the nodes close to attackers will receive more packets than they should and be considered as having a good capability in help forwarding packets.

Key Words: Network Coding Protocols, Wormhole Attack, Wireless Network & Packets

1. Introduction:

The increasing popularity and usage of wireless technology is creating a need for more secure wireless networks. Wireless networks are particularly vulnerable to a powerful attack known as the wormhole attack. This project researched and developed a new protocol that prevents wormhole attacks on a wireless network. A few existing protocols detect wormhole attacks but they require highly specialized equipment not found on most wireless devices. This project aims to develop a production against wormhole attacks that does not require as a significant amount of specialized equipment. In this new protocol, only a subnet of nodes requires a Global Positioning System (GPS), which enables the network devices to detect their own location. The thesis of this project suggests that the collaboration between GPS and non-GPS nodes can provide adequate detection of wormhole attacks in a wireless network. we focus on their impact and countermeasures in a class of popular network coding scheme - the random linear network coding (RLNC) system. In this system, in order to best utilize resources, before data transmissions, routing decisions are made based on local link conditions by some test transmissions. In this paper, we propose a distributed algorithm to detect wormhole attacks in wireless intra-flow network coding systems. The main idea of our solution is that we examine the order of nodes receiving innovative packets in the network, and explore its relation with a widely used metric, Expected Transmission Count (ETX), associated with each node. Our algorithm does not rely on any location information, global synchronization assumption or special hardware/middleware. It is only based on the local information that can be obtained from regular network coding protocols, and thus it does not introduce any overhead of extra test messages. The contribution of this paper is summarized as follows.

- ✓ We are the first to study the impact and countermeasures of wormhole attacks in wireless network coding systems.

- ✓ We investigate the harmful impact of wormholes on system performance and regional nodes resource utilization. We demonstrate the results via simulations on various scenarios.
- ✓ We use extensive experiments in various network settings, to verify that is effective (with over 89.43% detection rate), and efficient.

2. Related Works:

1. "DWAN: Defending Against Wormhole Attacks in Wireless Network Coding Systems", ShiyuJi, Tingting Chen, Sheng Zhong

In wireless network coding systems the routing and packet forwarding procedures are different from those in traditional wireless networks, the first question that we need to answer is: Will wormhole attacks cause serious interruptions to network functions and downgrade system performance? Actually no matter what procedures are used, wormhole attacks severely imperil network coding protocols. In particular, if wormhole attacks are launched in routing, the nodes close to attackers will receive more packets than they should and be considered as having a good capability in help forwarding packets. Thus they will be assigned with more responsibility in packet forwarding than what they can actually provide. Furthermore; other nodes will be correspondingly contributing less.

2. "Providing Immunity against Wormhole Attacks in Wireless Network Coding System" Irin Sherly S, Dhanalakshmi G

The centralized algorithm, which utilizes the ETX metric and the order of rank increment to detect wormhole attacks. In order to protect the validity of our method, we also introduce the public cryptographic scheme for the network. For each forwarding node in RLNC network, receiving the innovative packet will cause the rank of the previously received packets increase by one. We also find that the nodes with lower ETXs will be more likely to receive innovative packets (i.e., increase the rank) earlier than other nodes. On the other hand, wormhole links will make some nodes receive innovative packets (i.e., increase the rank) much earlier that they should. Thus, in the proposed centralized algorithm, we explore the order of rank increments in order to detect the wormhole links. Basically, in RLNC, when an innovative packet is sent from the source node, the nodes near the source node are more likely to receive the innovative packets earlier than the nodes that are far from the source node. Thus, the nodes with low ETXs can probably receive the innovative packets earlier.

3. "Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks" Yih-Chun Hu, Adrain Perrig, David B. Johnson

Introduce the notion of a packet leashes general mechanism for detecting and thus defending against wormhole attacks. A leash is any information that is added to packet designed to restrict the packet's maximum allowed Transmission distance. We distinguish between geographical leashes and temporal leashes. A geographical leash ensures that the recipient of the packet is within a certain distance from the sender to constructs a geographical leash, in general, each node must know its own location, and all nodes must have loosely synchronized clocks. When sending a packet, the sending node includes in the packet its own location, and the time at which it sent the packets. To use temporal leashes, when sending a packet, the sending node includes in the packet the time at which it sent the packet, when receiving a packet, the receiving node compares this value to the time at which it received the packet tr.

4. "Security vulnerabilities of network coding" M Gholibegi1, M Karimzadeh, D Moltchanov, Y Koucheryavy

Attackers belonging to this category introduce bogus links between network nodes and negatively affect the topology and link state knowledge of these nodes. Although the traditional security schemes such as packet leases and connectivity-based solutions can be used as countermeasures, their high computation and communication overheads make them inappropriate for network coding-based systems. Simply put, they decrease throughput of such systems absorbing the most important advantage of network coding. Designing security schemes to counter wormhole attackers ensuring proper link state and network topology information is quite challenging labor to overcome. To the best of our knowledge, security schemes that would be well-suited for wireless networks have not been proposed yet.

5. "A Survey: Detection and Prevention of Wormhole Attack in Wireless Sensor Networks" Akanksha Gupta & Anuj K. Gupta

Various routing protocols are existing for WSN. Some of the often used routing protocols are considered in this section and the risks of wormhole attacks to such protocols are described. These routing protocols are classified into two types: proactive / table-driven protocols and reactive / demand-driven protocols. AODV, DSR are reactive routing protocols and OLSR, DSDV and SEAD are proactive routing protocols. Protocol depends on symmetric cryptography and ensures that the source can authenticate each intermediate node in the route and the destination node authenticates the source. All intermediate nodes can eliminate or insert nodes in the list of nodes of the route request.

3. Existing System

Over View:

This chapter discusses previous work on preventing wormhole attacks. All protocols in this section fall under two broad categories: localization schemes and packet leashes.

A) Localization Schemes:

Localization systems are based on verifying the relative locations of nodes in a wireless network. Knowing the relative location may help conclude whether or not packets are sent by either a node or wormhole. Several localization schemes discussed in this section: Echo Protocol, Area-based Point Triangulation Test (APIT), Coordinate System, Signal Strength and Infra-Red (IR), and Directional Antennas.

RF (Radio Frequency):

Nodes in the regions of verification must prove they are part of the wireless network using radio frequency (RF) and ultrasonic sound capabilities. A verified node sends a RF signal to an unverified node in the network. To prove it is part of the network, the unverified node sends an ultrasonic signal back to the verified node. The verified node determines whether or not the unverified node is in the region of verification depending on the time it takes to receive an ultrasonic signal. RF signals are used in most wireless network devices today.

APIT (Area-Based Point in Triangulation):

An area-based point in triangulation test (APIT) which uses triangulation to determine the location of nodes in a network. Calculations are performed to check whether or not certain nodes are within triangles formed by anchors, which are nodes with Global Positioning System (GPS). These calculations determine the relative locations of all nodes in the network which may prove helpful to combating wormhole attacks. Compared to the Echo protocol, APIT does not require additional equipment for ultrasonic sound frequencies.

IR (Infra-Red):

Weaker signal strengths may indicate a node is farther away. However, signal strengths are not reliable outdoors because ambient sound can disrupt signals. IR is very efficient in pinpointing nodes in open spaces using invisible lasers. On the other hand, IR is very sensitive to its surroundings rendering it unusable outdoors due to the interference of sunlight and indoor areas which do not have a line-of-sight to each network device.

Using Directional Antennas:

Directional antennas are able to detect the angle of arrival of a signal. In this protocol, two nodes communicate knowing that one node should be receiving messages from one angle and the other should be receiving it at the opposite angle (i.e. one from west and the other at east). This protocol falls only if the attacker strategically placed wormholes residing between two directional antennas. This problem has been solved by having a verifier check on the communications between two nodes. However, some legitimate nodes are invalidated due to this solution. Drawbacks to this protocol include the flaw of rejecting valid nodes and requiring the use of directional antennas to prevent wormhole attacks.

B) Packet Leashes:

Protocols with packet leashes have been proven to be reliable wormhole attack detectors. Packet leashes place restrictions on a packet's maximum allowed transmission distance in a network.

Two Types of Packet Leashes:

- ✓ Temporal leashes
- ✓ Geographical leashes.

Temporal Leash:

Require tightly synchronized clocks on all nodes. Protocols based on temporal leashes ensure that packets transmitted across the network have an upper bound on its lifetime, which restricts the maximum distance of travel. Packets on a network remain valid for a certain time interval before they are rejected. However, setting up wormhole attacks under temporal leashes is difficult because packets must be sent through the wormhole within the restricted time period.

Geographical Leash:

Protocols based on geographical leashes differ slightly from temporal leashes in that each node must know its location and have loosely synchronized clocks. Using location and time, nodes can determine whether the packet is coming from a valid node or a wormhole. This protocol allows more flexibility in the synchronization time among nodes than temporal leashes. This type of packet leash also incorporates some of the same ideas used in localization schemes of using location to prevent wormhole attacks. A more refined temporal leash protocol known as the TESLA with Instant Key disclosure (TIK). TIK uses a hash tree to hold symmetric keys to authenticate nodes. Receiving nodes will be able to determine a packet's validity based on the time interval and the corresponding key of the sender node. TIK packets are structured so that the receiver node verifies the time interval and message authentication codes (HMAC) before the key arrives. If the time interval is valid, then the node verifies the key. Completing both tests would verify the sender was not a wormhole. The TIK temporal leash protocol effectively detects a majority of wormholes.

An attacker must know the right time intervals and keys pairs so that nodes in the wireless network will accept the wormhole's packet. Jamming attacks are much harder to counter and has more security problems. In this simplest form of jamming, the adversary interfaces with the reception of messages by transmitting a continuous jamming signal, or several short jamming pulses.

System Architecture for Existing System:

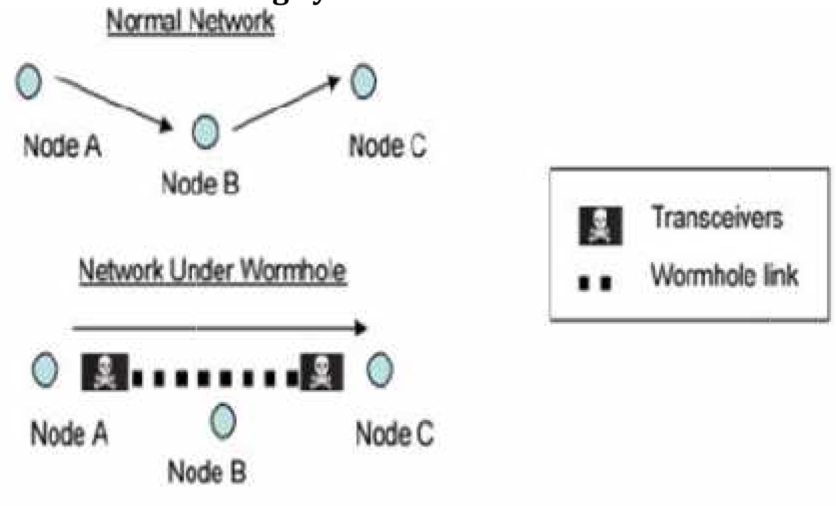


Figure 1: Set-up of a wormhole

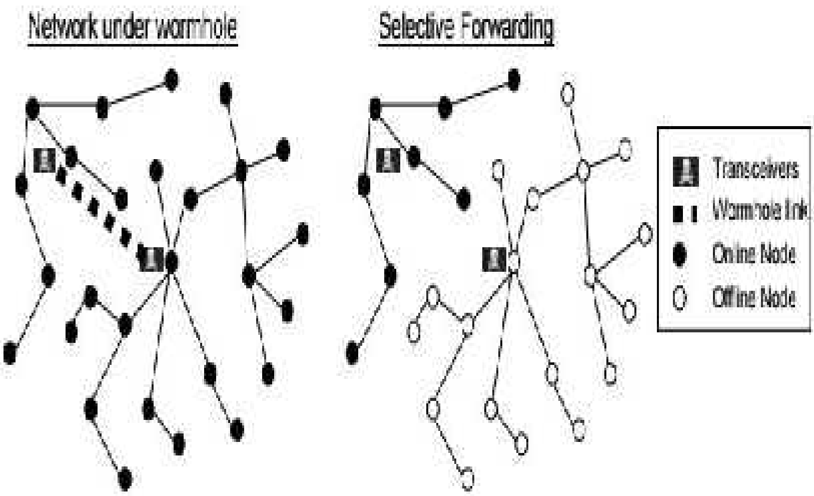


Figure 2: Selective Forwarding

Disadvantage:

- ✓ Errors in time difference must not be larger than a few microseconds or even hundreds of nanoseconds.
- ✓ Broadcast communication are particularly vulnerable under an internal threat model because all intended receives must be aware of the secrets used to product transmissions.
- ✓ The open nature of the wireless medium leaves it vulnerable to intentional interference attacks, typically referred to as jamming.
- ✓ The compromise of a single receiver is sufficient to reveal relevant cryptographic information.

4. Proposed System:

Overview of Proposed System:

In this section, we propose the centralized algorithm, which utilizes the ETX metric and the order of rank increment to detect wormhole attacks. In order to protect the validity of our method, we also introduce the public cryptographic scheme for the network. For each forwarding node in RLNC network, receiving the innovative packet will cause the rank of the previously received packets increase by one. We also find that the nodes with lower ETXs will be more likely to receive innovative packets (i.e., increase the rank) earlier than other nodes. On the other hand, wormhole links will make some nodes receive innovative packets (i.e. increase the rank) much earlier that they should.

Thus, in the proposed centralized algorithm, we explore the order of rank increments in order to detect the wormhole links. Basically, in RLNC, when an innovative packet is sent from the source node, the nodes near the source node are more likely to receive the innovative packets earlier than the nodes that are far from the source node. Thus, the nodes with low ETXs can probably receive the innovative packets earlier. However, the existence of wormhole link intuitively changes the normal network topology since the innovative packets can be transmitted through the wormhole link directly and safely, and thus the nodes around the remote side of the wormhole link can receive the novel packets earlier than expected.

Main Objectives & Mechanisms:

Attackers belonging to this category introduce bogus links between network nodes and negatively affect the topology and link state knowledge of these nodes. Although the traditional security schemes such as packet leases and connectivity-based solutions can be used as countermeasures, their high computation and communication overheads make them inappropriate for network coding-based systems. Simply put, they decrease throughput of such systems absorbing the most important advantage of network coding. Designing security schemes to counter wormhole attackers ensuring proper link state and network topology information is quite challenging labor to overcome.

Random Linear Network Coding (RLNC):

Linear Network Coding (LNC), especially Random Linear Network Coding (RLNC), owns numerous applications .Linear network coding permits each node in the network to pass on the combinations of the received data, in order to optimize the information capacity. Let r1; r2; ; rn denote the received data and the s will be the encoded data to be passed to another node. We obtain the combination f based on received data based on Equation (1). s = f(r1; r2.... ; rn) (1) For RLNC, f in Equation (1) is a random linear combination in the field GF(2k). f(r1; r2; ...; rn) =ΣN i=1E1R1 (2) An innovative packet must contain at least one basis that the node has not received, and the arrival of an innovative packet will increase the rank of the received packets by one. When the destination receives innovative packets, whose vectors are linearly independent from each other, it can restore the source information S based on the received data R. S = C−1R (3) Here C is the matrix of the coefficients of the received packets. Since each received packet is essentially a linear Combination of the original packets from the source, we can perfectly restore the original messages by multiplying the inverse of C.

Expected Transmission Count (ETX):

ETX has extensive applications in network coding systems. In this paper, the ETX of a node u in the network coding system denotes the expected total number of transmissions (including retransmissions) that the source node should make, in order to make the node receive one innovative packet in success. Node of high ETX means it is difficult to make it heard from the source, usually because the node is far from the source and the links between them are very loss. Thus, the metric of the ETXs is a good representation of the network structure. In existing works the ETXs are calculated based on the probabilities of packet loss between each pair of the nodes in the network.

Let u and v be two nodes, and p(u v) be the probability of successful transmissions between node u and v. For simplest case, if the network only has a sender u and a recipient v, then the ETX of the sender u is 1.0, and the ETX of v is shown as Equation (4) ETX(v) = 1/p(u v) (4)

Protocol Design:

This protocol adopted several design decisions to meet certain goals. These goals were to design a protocol that not only prevents wormhole attacks but also:

- ✓ Avoids using strict clock synchronization.
- ✓ Limits the need for specialized equipment.
- ✓ Ensures information confidentiality.
- ✓ Provides high performance, low power consumption and minimal memory storage.

Using strict clock synchronization to detect wormhole attacks is impractical. It requires all nodes to synchronize within a few microseconds or hundreds of nanoseconds, which involves the use of highly sensitive and expensive network devices. While providing protection against wormhole attacks is the primary goal, this protocol has secondary goals to provide information confidentiality and integrity in addition to performance, power conservation and minimal data storage.

Design of the Network and Network Devices:

Network Devices:

The most significant difference between GPS and non-GPS nodes is that non-GPS nodes do not know their location directly. They rely on neighboring GPS nodes to determine their relative location. Otherwise, GPS and non-GPS nodes share many similar attributes. They use asymmetric and symmetric key cryptography and store a neighbor list and their transmission range distance in their memory. Both types of nodes make use of asymmetric and symmetric key cryptography. Asymmetric key cryptography allows nodes to authenticate or verify the sender of the message since all GPS nodes are the same, only one public key need to be preloaded into each node's memory to verify the identity of a GPS node. In addition to holding keys for cryptography, each node maintains a neighbor list. This neighbor list consists of all GPS or non-GPS nodes within the transmission radius.

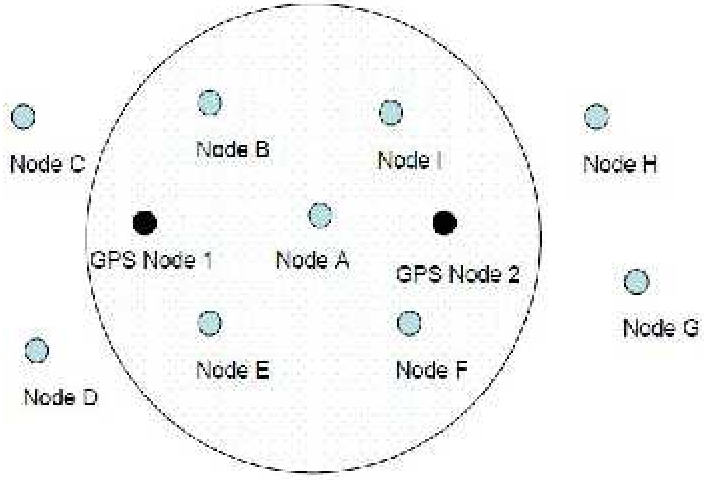


Figure 3: Neighbor List

Network Environment:

The network environment requires that each non-GPS node must be in the transmission radius of at least one GPS node to prevent wormhole attacks effectively.

However, the placement of nodes within the network does not matter. The network should work under ad-hoc or spontaneous networks. It should also work whether nodes in the network are mobile or stationary.

Protocol Functionality:

The design of this protocol relies on the collaboration of GPS and non-GPS nodes in the network. The following subsections will explain the initialization, communication and detection process of the protocol to identify wormhole attacks.

Initialization Process:

Before the initialization process, all nodes are either sleeping or powered off. When the nodes are powered, the first step of the protocol is for the GPS node to broadcast or announce its presence in the network. GPS nodes will send this signal encrypted with a private key within its fixed transmission radius. All nodes within that radius will wake up, decipher the message using the GPS's public key, and respond to the broadcast using an encrypted message with their own identity. After all the nodes have responded, each node will have compiled a neighbor list of GPS or non-GPS nodes around their transmission radius. This list is stored in each node's memory. Messages sent across the network include a nonce or random number generated depending on time of the message. These nonce are verified by the receiving node to ensure that they are not replays of previous messages. Without nonce, a wormhole attack can flood the network with messages to overwhelm the network. This type of attack is also known as a Denial of Service (DoS) attack which is commonly used to bring down the services of websites by overloading it with service requests. Nonce prevents attackers from replaying previous messages and nodes from accepting these messages because only nonce with the appropriate time stamps reaccepted.

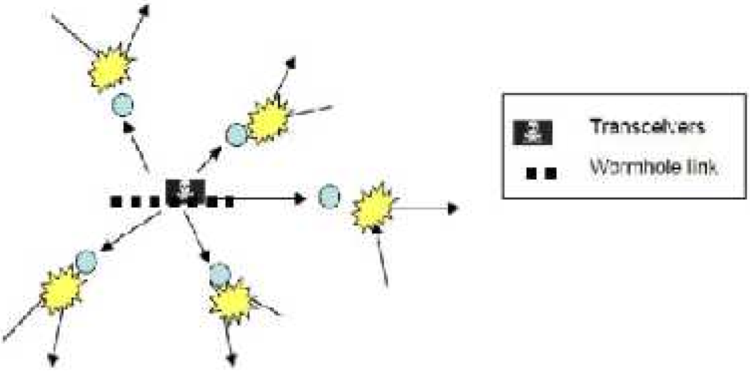


Figure 4: Denial of Service (DoS) Attack

Communication Process:

After the initialization process, all nodes should be able to forward messages to each other. To keep the communication confidential, each node encrypts its own message before sending it out to the network. As mentioned in section B, each node uses symmetric keys. Nodes in the network should remain in the communication state unless the one of the following conditions becomes true:

- ✓ One or more nodes move to a different location of the network.
- ✓ One or more nodes suddenly turn off or stop responding, requiring their removal from the network.
- ✓ One or more nodes suddenly turn on or arrive, requiring their addition to the network.

- ✓ The network has set a refresh rate that automatically brings the protocol back to initialization to update the network.

If one or more of these states becomes true, the protocol goes back to the initialization state to update each node's neighbor lists. Mobile networks may need to update at faster rates due to the constantly changing network structure. Higher refresh rates may help detect and prevent wormhole attacks but there are trade-offs in network performance and power consumption.

Advantages:

- ✓ Relatively Easy to Actualize by Exploiting Knowledge of the Network protocol and Cryptographic Primitives, extracted from Compromised nodes.
- ✓ Achieving strong security and prevention of network performance degradation.
- ✓ Jamming Attacks can be more easily Encountered and treated.

5. System Architecture:

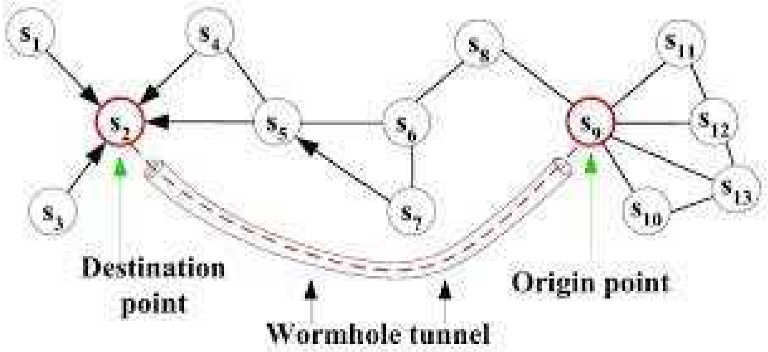


Figure 5: System Architecture

Internal Section:

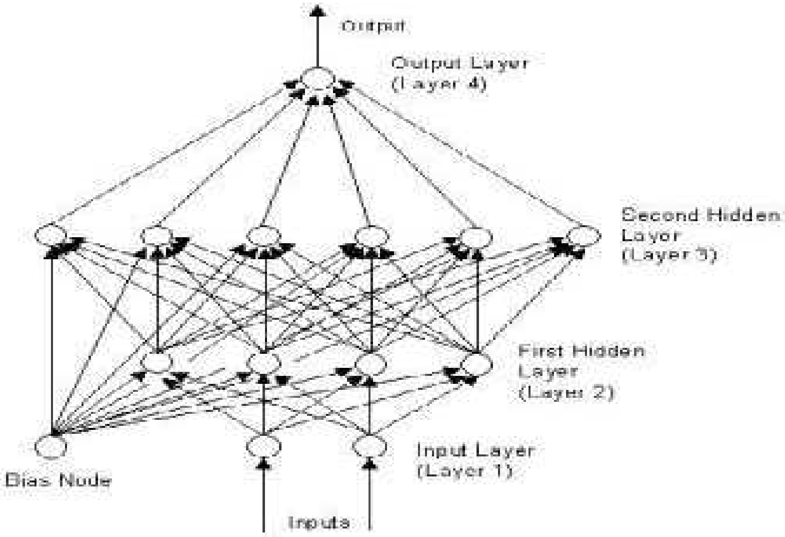


Figure 6: Internal Architecture

System Architecture Description:

Routing Protocols and Wormhole Attack:

Various routing protocols are existing for WSN. Some of the often used routing protocols are considered in this section and the risk of wormhole attacks to such protocols is described. These routing protocols are classified into two types:

- ✓ proactive / table-driven protocols
- ✓ Reactive / demand-driven protocols.

AODV, DSR are reactive routing protocols and OLSR, DSDV and SEAD are proactive routing protocols.

A) OLSR (Optimized Link State Routing):

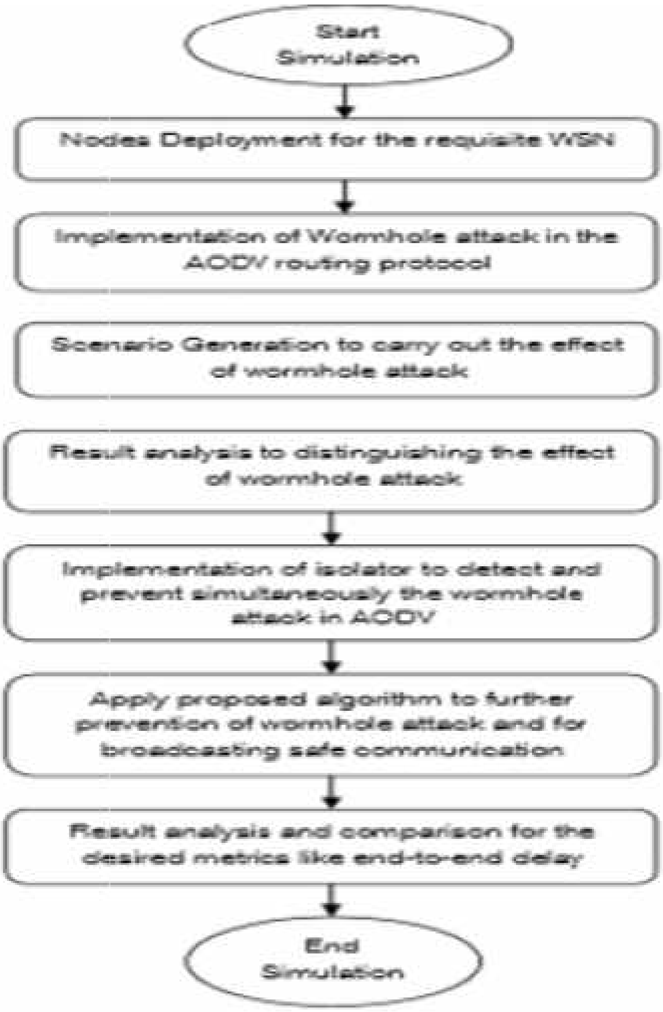
It is a proactive routing protocol in which information of the topologies get exchanged periodically. Hello messages are transmit to determine single hop neighbors. To allocate signaling traffic, flooding system is use. In this system each node forwards flooded message that was not forwarded by them earlier. The topology messages contain all the information about link states that are sent to all other nodes. With the help of this information, partial topology graph are obtained by every node after calculating the shortest path using symmetric relations.

B) DSDV (Destination Sequenced Distance Vector):

It is a proactive routing protocol, in which all the metric, destination routes, sequence number generated by the destination node and next hop to each destination are maintained in a table. Every node in the network acts as a router and table gets updated periodically by exchange of messages among neighboring routers. This protocol is open to wormhole attacks.

C) DSR (Dynamic Source Routing):

It is a reactive routing protocol because it discovers the required routes only after it has packets to transmit to the destination. It wants source route maintenance because during the utilization of the route, it is necessary to check the operation of the path and to report the sender regarding the errors. It is at risk to wormhole attack and denial of service attack at the destination.


Start Simulation
Nodes Deployment for the requisite WSN
Implementation of Wormhole attack in the AODV routing protocol
Scenario Generation to carry out the effect of wormhole attack
Result analysis to distinguishing the effect of wormhole attack
Implementation of isolator to detect and prevent simultaneously the wormhole attack in AODV
Apply proposed algorithm to further prevention of wormhole attack and for broadcasting safe communication
Result analysis and comparison for the desired metrics like end-to-end delay
End Simulation

D) SEAD (Secure Ad-hoc Distance Vector):

This protocol depends upon on one-way hash chains rather than asymmetric cryptograph and protects the network from uncoordinated attacks and Dos attacks. Several nodes have the ability to authenticate all other elements of the chain. This requires authenticating the metric of the routing table and the sequence number.

E) AODV (Ad-hoc On-demand Distance Vector):

It is an on-demand routing protocol which broadcasts RREQ messages to its immediate neighbors for sending messages to final destination and in turn these neighbors rebroadcast them to their neighbors. This whole process continues unless until the RREQ message reaches the destination.

Experimental Results:

The proposed energy efficient algorithm is implemented with Network Simulator. We have a RLNC simulation and Figures demonstrate the orders of rank increments with and without wormhole link. Here we have 100 nodes in the network, and we run Algorithm to calculate the ETXs. In the figures, the red curve denotes the ascending ETXs of the nodes. Then we start the network coding transmission. The source node sends out an innovative packet, and for each node, receiving the innovative packet will result in rank increment from 0 to 1. We collect the time stamps of rank increments on the nodes during the whole transmission, and find out the time order of rank increments. That is the blue line, which denotes the ETXs of the nodes based on the ascending time order of rank increments.

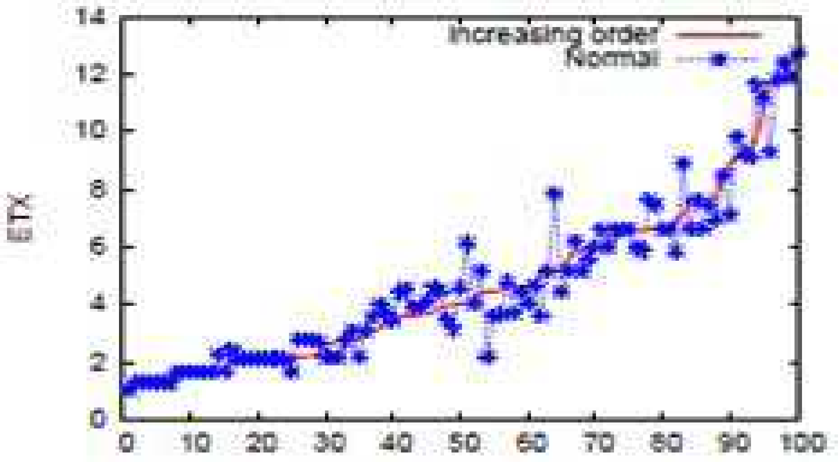


Figure 7: Order of rank increment

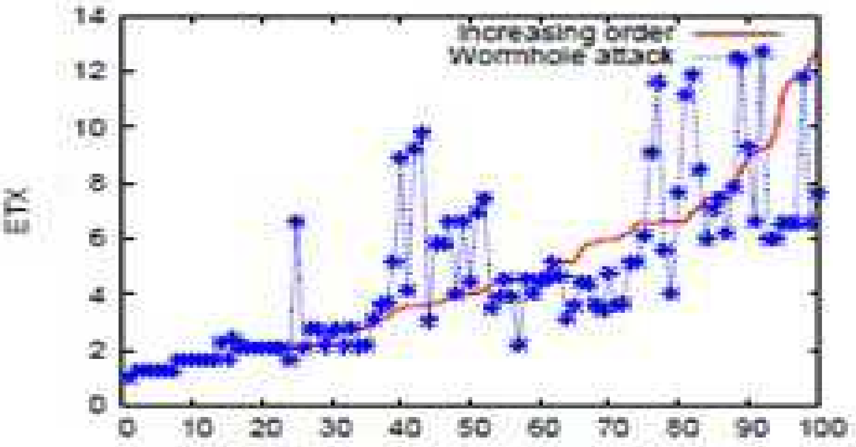


Figure 8: Order of rank increment

We find that the blue line deviates from the red line when the wormhole link exists. For the centralized algorithm, we set up a central node, which owns the authority to gather information from all the nodes in the network, and we run a wormhole detection algorithm based on the rank increasing information on the central node. Each node is responsible to record the time when the rank of the received packets increases and then generates a report, which includes the details such as the time, the node address, and the rank. Each node delivers the reports to the central node via common unicast. At last, we update the bound of the distance for the next detection, in order to make our algorithm adaptive.

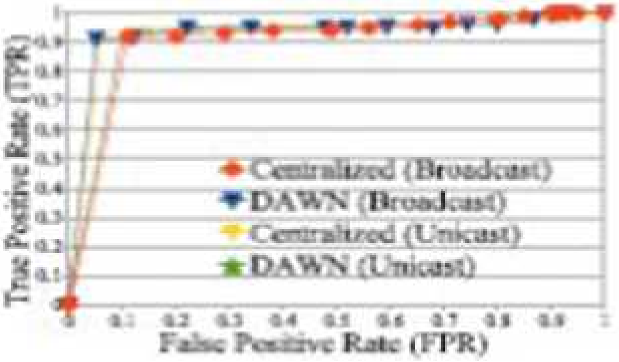


Figure 9: The ROC diagram of Centralized Algorithm and DAWN

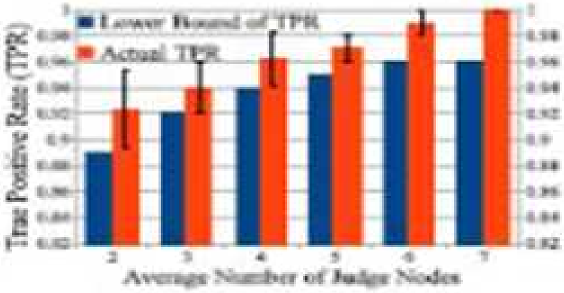
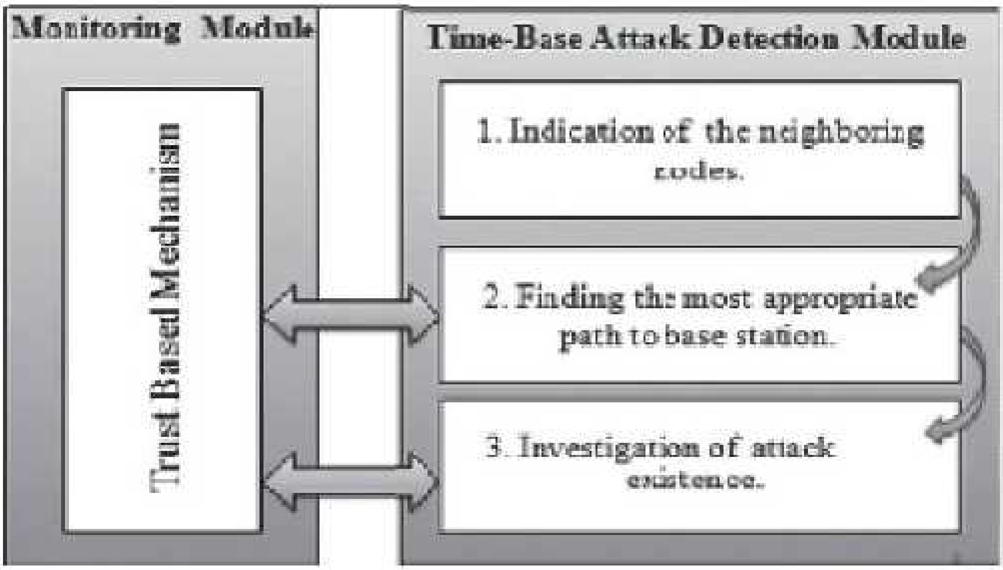
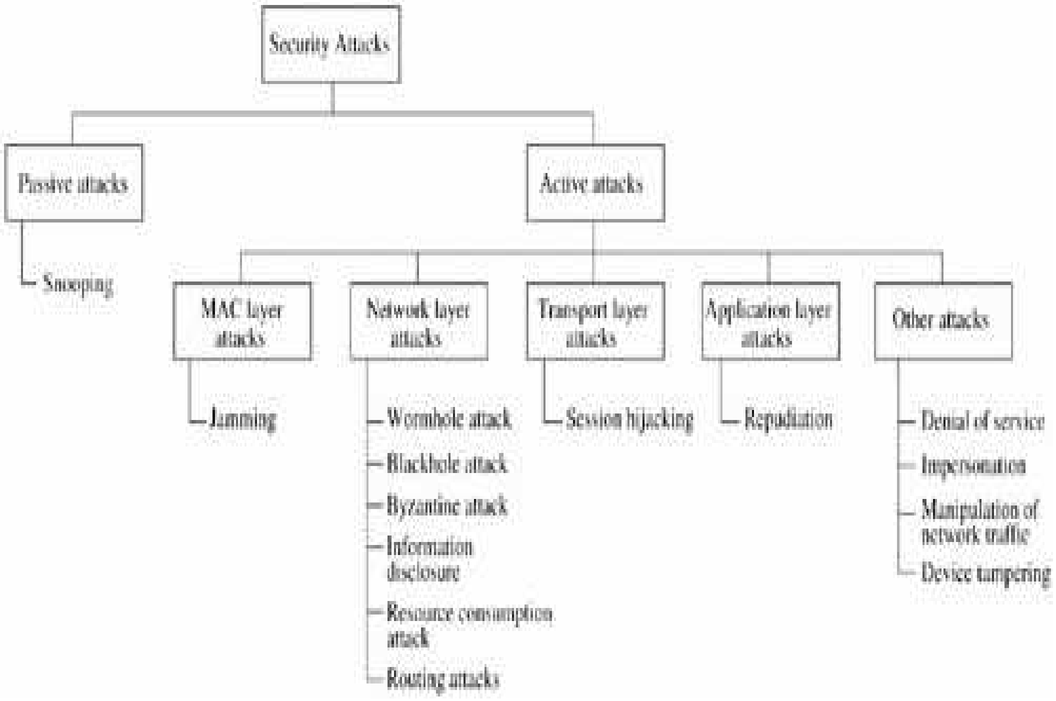


Figure 10: The TPR increases as the number

Functions of System Design:


Monitoring Module
Trust Based Mechanism
Time-Base Attack Detection Module
1. Indication of the neighboring codes.
2. Finding the most appropriate path to base station.
3. Investigation of attack existence.



Two experiments were conducted to verify the effectiveness of the protocol. These experiments show whether the protocol design could work on wireless networks with the following conditions:

- ✓ Limited numbers of GPS nodes
- ✓ Large network areas
- ✓ Ad-hoc or randomized networks

Used Mechanisms:

- ✓ The centralized algorithm
- ✓ The distributed detection algorithm

In this section, we consider a scenario where a central authority cannot be found. We propose a distributed algorithm to detect wormhole attacks in wireless network coding systems. The basic idea of DAWN is that any two nodes in the neighborhood, the one with lower ETX is supposed to receive novel packets earlier than the other one with high probabilities. In other words, innovative packets are transmitted from low ETX nodes to high ETX nodes with high probabilities. In particular, DAWN has two phases on each node:

- ✓ Report packets direction observation results to its neighbors and
- ✓ Detect whether any attackers exist .The Detect phase is based on the received results from neighbors during the Report phase.

6. Future Enhancement:

Future wireless networks are expected to provide high speed internet access anywhere and anytime. The popularity of iPhone and other types of smart-phones undoubtedly accelerates this trend and creates new traffic demand. The current cellular broadband wireless technologies are unable to meet increasing demands for data rates, coverage, novel services and user numbers. Network coding has emerged as a promising tool for the design of future wireless networks. In this proposal, we systematically design novel network coding schemes for future wireless cellular networks and related signal processing algorithms, capable of achieving significant improvements in network throughput, energy efficiency and reliability.

7. Conclusion:

Network coding is a new tool of both theoretical and practical importance. Network coding enables more efficient, scalable, and reliable wireless network. These opportunities come with a need for re-thinking our MAC, routing, and transport protocols. Today's wireless systems are not equipped to meet the demands of emerging high bandwidth applications. The dissertation advocates an alternative architecture built around network coding and shows that it can provide large throughput and reliability gains. We conclude by examining the benefits of our network coded wireless architecture and the remaining challenges the combination of wireless network and protocol coding system is highly secured and it defending against wormhole attacks in efficient manner.

8. References:

1. S. Ji, T. Chen, S. Zhong, and S. Kak, "Dawn: Defending against wormhole attacks in wireless network coding systems", IEEE Conference on Computer Communications- 2014.
2. Irin Sherly. S, Dhanalakshmi. G, "Providing Immunity against Wormhole Attack in Wireless Network Coding System" in IJIRCCE.vol.3, Feb 2015.
3. Yih-Chun Hu, Adrian Perrig, David B. Johnson, "Packet Leashes: A Defense against wormhole Attacks in Wireless Networks", IEEE INFOCOM-2003.
4. M. Gholibegi, M. Karimzadesh, D. Moltchanov, Y. Koucheryavy, "Security Vulnerabilities of Network Coding" Issue 1 version 1.0 year-2010.
5. Akanksha Gupta & Anuj K. Gupta, "A Survey: Detection and prevention of wormhole Attack in Wireless Sensor Networks", Volume 14 Issue 1 version 1.0 year 2014.
6. S.R.D.R. Maheseswari, J. Goa, "Detecting Wormhole Attacks in Wireless Networks is using Information", in IEEE INFOCOMM. 2007.
7. Y-C, HU, A Perrig, and D,B. Johnson, " Wormhole Attacks in Wireless Networks", IEEE Journal on Selected Areas in communications, vol.24, no.2, 2006.
8. Khin Sandar Win, "Analysis of Detecting Wormhole Attacks in Wireless Networks", World Academy of Science, Engineering and Technology, 2008.
9. A.Vani, D. Sreenivasa Rao, "A Simple Algorithm for Detection and Removal of Wormhole Attacks for Secure Routing In Ad Hoc Wireless Networks", IJCSE, June 2011.
10. J. Le, J. C. S Lui, and D. M. Chiu, "DCAR: distributed coding-aware routing in wireless networks", In Proc. IEEE Trans. Mob. Comp, V.9, N.4, pp.596-608, Apr.2010.