2008

Attacks and countermeasures on routing protocols in wireless networks

Narasimha Rao Venkata Laxmi Velagaleti
Iowa State University

Attacks and countermeasures on routing protocols in wireless networks

by

Narasimha Rao Velagaleti

A thesis submitted to the graduate faculty

in partial fulfillment of the requirements for the degree of

MASTER OF SCIENCE

Co-majors: Computer Science; Computer Engineering

Program of Study Committee:
Johnny S. Wong, Co-major Professor
Julie A. Dickerson, Co-major Professor
Wensheng Zhang

Iowa State University

Ames, Iowa

2008

DEDICATION

I would like to dedicate this thesis to my parents.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ACKNOWLEDGEMENTS

I would like to take this opportunity to express my thanks to those who helped me on the aspects of research pertaining to this thesis. First and foremost, Dr.Johnny Wong for his guidance, motivation and support throughout the research. His creative insights have often encouraged me and renewed my interest in the research field. His weekly research paper presentation sessions helped me a lot in exploring various fields related to my research. He also helped me in planning and organization of my study which allowed me to finish the research work on time. I sincerely thank my co-major professor Dr. Julie A. Dickerson for her constant support and invaluable suggestions. I greatly appreciate her for supporting me with an assistantship for my MS program. I would also like to thank my committee member Dr. Wensheng Zhang for his invaluable ideas. I am grateful to Xia Wang for her wonderful ideas and critical suggestions. I would also like to thank Wei Zhou for his timely help in running simulations. I am thankful to Vikram Koundinya, Abhishek Sinha, Neevan Ramalingam, Anurag Sharda and Abrar hasan for all their help in proof reading and matlab help. I would like to acknowledge each and everyone in my research group for their participation in my research presentations.

Last but not the least, I would like to thank my parents for their constant love, support and encouragement.

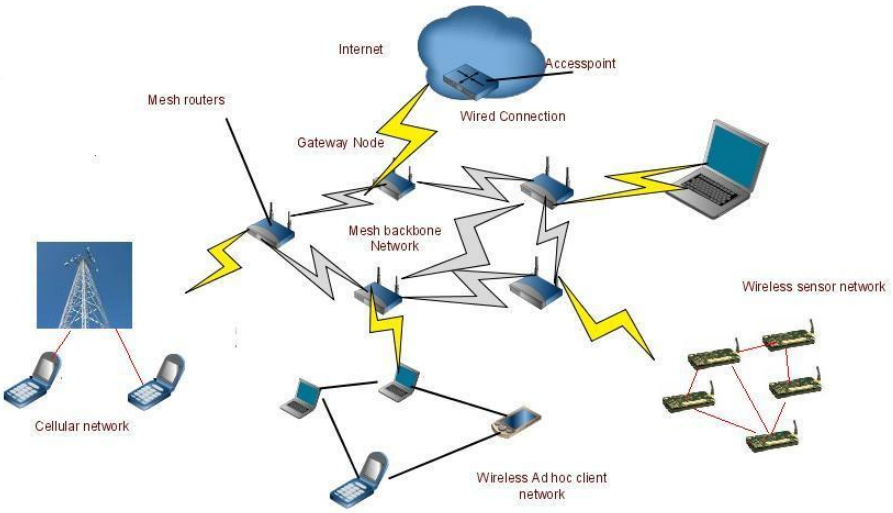
CHAPTER 1 OVERVIEW

1.1 Introduction

Wireless networks have certainly been a revolution in today's technological world, ranging from traditional cellular networks to mesh networking and vehicular ad hoc networks. In one way, wireless networks can be classified into two modes namely infrastructure and ad hoc modes. In infrastructure mode, nodes are wirelessly connected to one or more access-points which inturn are connected to wired Ethernet cables. Infrastructure wireless networks are centralized, scalable and easily manageable in terms of security and reachability. They are more expensive than ad hoc networks due to additional access-point hardware. Ad hoc wireless networks are decentralized in a sense that the nodes themselves forward data to other nodes without any access-point in between. Nodes in a wireless ad hoc network communicate directly. Ad hoc networks are not scalable. Of late, most of the research communities, academia and industry have been shifting their focus toward wireless mesh networks (1)(3). In this study, wireless ad hoc and wireless mesh networks are discussed and dealt with respect to attacks on security and reliability along with possible countermeasures. Wireless mesh networks can be considered as mixed mode wireless networks as they are both infrastructure and ad hoc in nature. Wireless mesh backbone network is ad hoc in nature and a few of the mesh nodes act as gateways to the access points that connect to Ethernet. See figure 1.1. Wireless mesh networks have the potential to provide the most reliable, faster and cheaper ways of networking compared to traditional wireless networks. In this thesis, mainly ad hoc nature of wireless mesh networks is discussed in the context of routing, security, reliability, attacks and countermeasures.

Most network models and protocols so far have been designed based on single radio paradigm where each wireless node is equipped with a single radio. These networks suf-

Figure 1.1 **A Heterogeneous Wireless mesh network**



fer from poor system throughput as a node having a single radio interface cannot transmit and receive simultaneously. Capacity constraints (9)(BelAir) are also very vital in wireless mesh networking or community networking in general because of the inevitable interference between simultaneous transmissions. IEEE 802.11 standard has introduced the concept of non-interfering orthogonal channels to improve the capacity (4)(5)(6) in multi-hop wireless networks. To improve the overall network throughput and channel utilization, nodes are equipped with multiple radio interfaces, operating on different channels allowing them to transmit and receive simultaneously.

Though multi-hop multi radio paradigm (BelAir) is gaining importance these days, there are still some challenges such as synchronization amongst neighbors, optimal channel assignment and most importantly routing. An ad hoc routing protocol is an agreement amongst nodes as to how they control routing packets amongst themselves. The nodes in an ad hoc network discover routes as they do not have any prior knowledge about the network topology. In general, there are many routing protocols (10) designed and devised for wireless ad hoc networks. Routing protocols in ad hoc networks are primarily classified into two types. They are 1. Proactive routing protocols 2. Reactive routing protocols. Proactive routing protocols are

table driven routing protocols. The routes are updated continuously and when a node wants to route packets to another node, it uses an already available route. Destination sequenced distance vector routing protocol(DSDV)(11), Optimized link state routing protocol (OLSR)(12), Wireless routing protcol(WRP)(13), etc. fall under the category of proactive routing protocols. In reactive routing protocols, when there is a need to route packets from one node to another, then the routes are determined on demand between those two nodes. These routing protocols are also called ondemand routing protocols. Dynamic source routing protocol(DSR)(8), Ad hoc On Demand Distance Vector (AODV) protocol, Microsoft research-link quality source routing protocol (MR-LQSR) (5), etc. come under the category of reactive routing protocols. In source routing protocols, the source node determines the best route to destination. In link quality based routing, routing decisions are based on the value of link quality routing metric. Wireless ad hoc routing protocols such as DSR (8) use Hop-count as the routing metric. But, Hop-count is the least performant and is also not suitable in multi radio paradigm as it does not take the advantage of channel diversity. Authors of (4) designed a new metric called ETX (Expected Transmission count) that takes link quality metrics into account, unlike Hop-count. ETX was mainly designed for single radio paradigm and hence does not account for channel diversity. Authors of (5) have introduced a metric called WCETT (Weighted Cumulative Expected Transmission Time) that takes channel diversity and also available bandwidth factor into account, unlike Hop-count and ETX, and is implemented in Microsoft's Wireless Mesh Network toolkit as the routing metric. Authors of (7) believe that the WCETT metric may not reflect the right level of channel diversity. They proposed a new metric called AETD (Adjusted expected transfer delay) that takes ETT and delay jitter between consecutive packet transmissions into account, that might reflect the actual level of channel diversity. In their simulations, this metric outperformed WCETT, ETX, HOP on most occasions. More information about these metrics will be presented in the subsequent sections. None of the metrics has captured the effect of ETT on the entire path. In this work, a link quality based routing metric called Variance based path quality metric(VBPQ) has been proposed, evaluated in terms of reliability and security, and compared to other metrics. Previous works (5)(7) mainly considered the impact

of channel diversity and the link quality (in terms of bandwidth and the loss rate) on routing but not much on security aspects. There is another sect of routing protocols classified as secure routing protocols. Authenticated Routing for Ad hoc Networks (ARAN) (15), Secure AODV (16)etc. are a couple examples of secure routing protocols. These protocols provide security by employing various cryptographic techniques. There are some attacks like wormhole attack (19), where only cryptographic techniques are not sufficient to detect the attack. Crytographic techniques provide security at the cost of some performance overhead. This study proposes a new denial of service attack known as delay-variation attack (a variation of blackhole attack) and also discusses its possible countermeasure. The new routing metric VBPQ itself is able to detect the attack with minimal overhead. For this, the network model can be any ad hoc network and in particular wireless mesh back bone network. Next, a possible countermeasure for wormhole attack in a wireless ad hoc network, where each node in it executes link quality based source routing protocol, is proposed . So far, wormhole attack detection for link quality based routing protocols has not been discussed in the earlier literature. In this paper, a data mining approach which will be discussed later was employed to detect wormhole attacks in wireless ad hoc networks based on link quality source routing protocols.

1.2 Motivations

This study has two motivations.

1.2.1 Motivation A:

In (4), the authors introduced a new link quality based routing metric called expected transmission counts (ETX). Higher the value of ETX of a link, lower is the link's quality and lower the ETX value, higher is the link quality. The authors of (5) came up with a similar notion of link quality metric known as expected transmission time (ETT). Basically, ETT is bandwidth adjusted ETX. In a similar fashion, one can infer that higher the value of ETT, lower is the link quality. Metrics such as WCETT (5) and AETD (7) take total ETT of a route and channel diversity into consideration. They do not consider the impact of ETTs of

individual links in a route. Due to this, an attacker can intentionally create contention in some of the links and offering better quality on some other links so that it makes no difference in the value of overall path quality metric (Total ETT). This type of attack may hamper the performance of the entire network and may also result in other attacks like wormhole, gray hole and blackhole attacks. This is the basic motivation behind proposing a reliable and secure routing metric VBPQ.

1.2.2 Motivation B:

Wormhole attacks are very easy to deploy but hard to detect and prevent. A wormhole is a tunnel that connects two distant points in a wireless ad hoc network. A tunnel can be anything like a low latency wired connection, a wireless link that has a large transmission range etc. The data at one end is replayed at the other through one of these possible virtual links. There have been many detection and prevention techniques discussed in the literature (19) (21)(20)(22). In (22), the authors used location based detection mechanism to detect the attack. Hopcount is estimated between two nodes based on the distance between them. This works well when the routing protocols use hopcount based metrics. This is not the case if the routing protocols are link quality based. This is the motivation behind proposing a new method of detecting wormhole attacks in link quality based routing protocols.

1.3 Problem Statements

This study discusses two problems mainly concentrating on the issues of security and performance in wireless ad hoc and mesh networks. Also a few possible attacks on routing and their possible countermeasures have been proposed.

1.3.1 Problem statement A:

The metrics such as WCETT and AETD have failed to capture the actual effect of ETTs of individual links of a path leading to delay variation attack. This attack not only hinders the security of the system but also reduces the performance of the network. To avoid this, a new,

reliable, robust and secure routing metric known as VBPQ has been proposed and discussed in this work. This type of metric is suitable to route packets in a mesh network as one of the main properties of a mesh network is its reliability.

1.3.2 Problem statement B:

There are a few techniques that tell us about detecting and preventing wormhole attacks in wireless ad hoc networks based on hopcount based routing protocols. There are some other techniques like leashes that use synchronization primitives to detect wormhole attacks. But there are no detection or prevention techniques to detect wormhole attack when the underlying protocol is link quality based routing protocol. To fill this gap, this work discusses a well known data mining approach to detect wormhole attack in wireless networks based on link quality based source routing protocols.

1.4 Contributions

There are mainly two main contributions this study addresses.

1. A secure and reliable routing metric for multiradio link quality based source routing protocols (VBPQ). VBPQ

a. favors the path that has less deviation from the Average ETT (AETT) of the entire path (less variance and more reliable path), if two paths have the same AETT or the same AETD or the same WCETT value.

b. achieves whatever AETD or WCETT can achieve and also adds some extra robustness to the routing mechanism without creating any imbalance between security and performance of the entire system while adding security to the routing mechanism.

c. prevents a possible delay variation attack that is not even detected by WCETT or AETD.

d. is better in terms of security and performance when compared to ETX, ETT, WCETT and AETD. Simulation results show the performance evaluation of the metric.

2. A detection algorithm (WHDETECT) that detects wormhole attack in wireless ad hoc networks based on link quality based source routing protocols. The algorithm calls a subroutine

that does a cross feature analysis technique which is a data mining technique proposed in (23).

1.5 Thesis outline

The rest of the thesis is organized as follows

1.5.1 chapter 1:

In chapter 1, an overview on this work has been provided. A brief introduction on wireless ad hoc networks and mesh networks was given. In this chapter, the motivation behind this study has been provided along with the problem statements and contributions of this study. This chapter briefly described the need to proposing a new routing protocol VBPQ and how this protocol may help avoiding certain attacks on routing mechanism. This chapter also discusses a little bit about wormhole attack and its countermeasure algorithm.

1.5.2 chapter 2:

In chapter 2, review of literature, related and background work for this thesis is presented. It talks about wireless mesh networks and a few challenges related to mesh networks. It discusses the need of multi radio multi hop wireless networks. It also presents some of the challenges to be met in routing in wireless ad hoc networks. It discusses and compares various routing protocols for wireless ad hoc networks. This chapter also explains in detail some of the routing metrics that formed the basic foundation for proposing a new link quality based metric. It also talks about the need of data mining approaches in detecting anamolies and attacks. This chapter presents a well known data mining approach and explains how this method is going to detect wormhole attacks in link quality based routing protocols.

1.5.3 chapter 3:

This chapter mainly covers the actual contributions of this thesis. It talks about this newly proposed metric VBPQ and explains how this metric is able to achieve a few things which WCETT or AETD may not achieve. It also talks about an attack scenario and explains how

VBPQ routing metrics helps in preventing such an attack. As a second part of this chapter, an algorithm for detecting wormhole attacks in link quality based routing protocols is provided. In this algorithm, a well known data mining approach known as cross feature analysis is used. This chapter also describes the selection criteria for the features to be used in the algorithm.

1.5.4 chapter 4:

This chapter presents results section. In this section, metric VBPQ is evaluated against WCETT, AETD and ETX under multi radio and single radio scenarios. Qualnet 4.0 was used as the simulation platform. A new evaluation metric 'power' which is equal to the ratio of throughput and delay has been introduced and every metric is evaluated based on the value of the 'power'. In the implementation subsection of this chapter, some of the implementation details of wormhole attack detection are explained. Recall-Precision graphs for various number of features are plotted and compared.

1.5.5 chapter 5:

This chapter talks about the future work and conclusions.

CHAPTER 2 REVIEW OF LITERATURE

This section covers a brief review of literature on various concepts like wireless ad hoc networks, wireless mesh networks (wmns), challenges in wmns, different radio technologies. This section also discusses different routing protocols in wireless ad hoc networks, routing metrics used in routing protocols, comparison amongst routing metrics. Motivation behind proposing a new routing metric is provided. A brief note on routing attacks, countermeasures and use of data mining approaches in detecting routing anamolies is also included.

2.1 Background work

This section covers the necessary background knowledge to understand the rest of the thesis. In the next section, related work leading to the problem statements of this thesis is explained in detail

2.1.1 Wireless Ad hoc and Mesh networks

It is always fascinating to think about the evolution of the concept of wireless networks and its impact on today's technological world. Gadgets like remote controllers, radio transistors, cellular or mobile phones, laptops inbuilt with radio are very common these days. Especially mobile phone is the most widely spread technology today. People are gradually going for laptops rather than desktops and showing interest in wireless communication. Wireless networks are easily deployable and inexpensive as compared to wired networks where a lot of wiring is required to connect every computer. Wireless networks can be broadly divided into two categories namely wireless infrastructure networks and wireless ad hoc networks. In infrastructure networks, wireless clients basically connect to a wireless access point which is inturn

connected to a Ethernet cable that might connect to the Internet. A node communicates to every other node internally or externally via an accesspoint falling in the range of this node. Infrastructure wireless networks are centralized, scalable and easily manageable in terms of security and reachability. But they are more expensive than ad hoc networks due to additional accesspoint hardware. On the other hand, ad hoc networks are decentralized, small groups of wireless clients where each client communicates with other client directly or in a multi hop fashion. Ad hoc networks are not very scalable. The nodes in an ad hoc network do not have any prior knowledge of the network topology and therefore had to dynamically find the nodes they wish to communicate with. Every node in an ad hoc network agrees on a routing protocol to route packets. Security, performance and speed have always been very important challenges for wireless ad hoc networks. Ad hoc networking is a cross layer challenge. Choice of what technologies at all layers(physical, MAC, network, transport etc) are to be used does make an impact towards the performance of the system. Wireless mesh networking is undoubtedly the talk of the research world in wireless networks. These days researchers, academia, companies etc are intensifying their focus on WMN and developing products for providing an affordable and last mile broadband Internet service. If there is careful and proper planning of establishing mesh kind of infrastructure all over the world, there is no doubt that people in every nook and corner of the world shall gain access to the Internet at an affordable price. Many mesh products with different capabilities and enhancements have already made their mark in the market, but due to scalability, security and privacy issues WMNs are not yet widely deployed. There has been a lot of research taking place in this field and many researchers in their articles (1)(2)(3)(24) touched upon various aspects of wireless mesh networks. A lot of study is going on in the areas of routing techniques to be used, feasibility of WMNs in offices (25), scalability and implementation issues, and last but not the least security and privacy issues. The most important thing to note about WMNs is that it is a hybrid network which neither falls into the category of ad hoc networks nor into the category of infrastructure based networks. A properly designed wireless mesh network should be able to provide flexibility and inter-operability among different types of users, different types of heterogeneous networks such

as MANETs, wired networks, WiMax, wireless sensor networks, Cellular networks etc. To design a heterogeneous WMN architecture (See figure 1.1)that is able to satiate the needs of different classes (based on the type of usage) of people and mitigate the loss caused by attackers is not an easy job. Researchers have started to revisit the protocol design of existing wireless networks, especially of IEEE 802.11 networks, ad hoc networks, and wireless sensor networks, from the perspective of WMNs. Industrial standards groups are also actively working on new specifications for mesh networking (26). Some of the advantages of WMNs are self configurability, self healing, reliable, low deployment costs, highly integrated and heterogeneic network connectivity. Some of the key design issues of WMNs are scalability, radio technologies, mesh connectivity, quality of service, cross layer design, security and privacy issues. This thesis mainly focuses on multi radio paradigm, connectivity by means of a routing protocol and its impact on quality of service, performance and security. Advanced radio technologies such as cognitive radios, reconfigurable radios, multi-radio/ multi channel systems (routing in multi radio environment (5)), smart antenna systems etc. Even the power constraints for various devices taking part in the networking are different. So the design of MAC/ routing protocols must confirm to the requirements of these evolutionary radio technologies.

1. Single radio networks:

So far, routing protocols and upper layer protocols have been built on single radio MAC layer and physical layer paradigm. Radio technologies play a very important role in providing a better and faster service to a mesh user. With a rapid increase of user pool featuring in wireless communication, the capacity constraints stand vital in providing a better performance. Physical interference caused by wireless links in the interference range of one another, collisions due to simultaneous transmissions and receptions etc are some of the basic problems faced by the nodes in an ad hoc network. To improve the performance and capacity of a single radio ad hoc network system, authors of (6) had come up with a channel hopping technique based on the concept of orthogonal channels introduced by the 802.11 standard. These kinds of protocols incur a lot of synchronization overhead and communication overhead as the network scales but are promising in improving the capacity of the system and can be considered as an

alternate approach to having multiple radios on each node.

2. Multi radio networks

Capacity constraints (9)(BelAir) are vital in wireless mesh networking or community networking in general because of the inevitable interference between simultaneous transmissions. IEEE 802.11 standard has introduced the concept of non-interfering orthogonal channels to improve the capacity (4)(5)(6) in multi-hop wireless networks. To improve the overall network throughput and channel utilization, nodes are equipped with multiple radio interfaces operating on different channels which allows to transmit and receive simultaneously. This does not require any synchronization overheads possible in the technique SSCH proposed in (6). Having multiple radios on each node enables the network to use most of the radio spectrum and secondly the capacity of the forwarding nodes is not halved as in the case of single radio. Moreover, the prices of wireless cards are rapidly coming down. Providing multiple radios on each node undoubtedly opens affordable and promosing avenues for improving the capacity and performance of wireless ad hoc and mesh networks. Proper usage of radios in the network is determined by the term "'Channel diversity"'. Better is the channel diversity of a route better is the performance of the route.

In this thesis, experimental results show that for every protocol in comparison, use of multiple radios provide better performance than that of single radio case.

2.1.2 Routing protocols in wireless ad hoc networks

One of the most important and a difficult mechanism to maintain in ad hoc networking is the routing mechanism. An ad hoc routing protocol is nothing but an agreement amongst nodes as to how they control routing packets amongst themselves. The nodes in an ad hoc network discover routes as they do not have any prior knowledge about the network topology. In general, in a wireless ad hoc network the nodes have a list of forwarders who do the job of relaying or routing packets to their final destinations. Routing protocol semantics and packet structures decide how the packets are relayed and what and how the content is transfered from one node to another. In general, there are many routing protocols (10) designed and devised

for wireless ad hoc networks. Routing protocols in ad hoc networks are mainly classified into two types. They are

1. **Proactive routing protocols**
2. **Reactive routing protocols**

There is another class called hybrid routing protocols which is basically a mix of proactive and reactive protocols.

2.1.2.1 Proactive routing protocols

Proactive routing protocols are table driven routing protocols. The routes are updated continuously and when a node wants to route packets to another node, it uses an already available route. These protocols maintain routes to all possible destinations even though a few of the routes may not be needed. Every node in the network maintain tables of routes and when the network topology changes updates are sent across the network. These protocols require nodes to send control packets periodically to maintain the routes. To maintain all possible routes in a network is difficult because the control packets for route maintenance consume a lot of bandwidth on links where there is no need of data transfers. These protocols incur a lot of routing overhead. There are some really good advantages of proactive protocols. These protocols find routes very easily and thus the response time for the session to be started between the two end nodes in very less. Destination sequenced distance vector routing protocol(DSDV)(11), Optimized link state routing protocol (OLSR)(12), Wireless routing protcol(WRP)(13) etc. come under the category of proactive routing protocols. A brief description of protocol DSDV(11) is given below.

Destination sequenced distance vector routing protocol

- In this protocol, each node maintains a table of routing entries. Each entry contains destination's address, number of hops required to reach the destination and a sequence number given by the destination to indicate the freshness of the route. This protocol uses hopcount as the metric.

- Routing tables are updated whenever there are changes in the topology. There are two kinds of route updates namely full dumps and small incrementals. Full dumps are infrequently transmitted route updates that carries entire routing table information. Small incrementals are frequently transmitted control packets that carry only the changed information since the last full dump. Additional tables are maintained to store the information carried by these small incrementals.

- Sequence number is the first selection criterion used to select a route. A fresh route is preferred. If there are more than one route with the same sequence number, then the route with the lowest cost (hop count for example) is selected. DSDV, which is an improvement over Bellman-Ford routing algorithm (29) is not very scalable.

2.1.2.2 Reactive routing protocols

In reactive routing protocols, when there is a need to route packets from node to another, then the routes are determined ondemand between those two nodes. These routing protocols are also called ondemand routing protocols. In this the source node initiates the route discovery phase. In a way, these protocols are also called as source routing protocols. There are basically two stages in reactive routing mechanism after the node desires to send data to the destination. First stage is called Route discovery stage. In this stage, the source node broadcasts Route Request messages and are spread across the entire network. Routes are added to the list once the Route Reply packets originated from the destination reach the source via various forwarders. Source selects the route based on the metric used and the routing semantics. Once the route is established, data transfer takes place. Data transfer and route maintenance go hand in hand in the second stage. Dynamic source routing protocol(DSR)(8), Ad hoc On Demand Distance Vector (AODV) protocol, Microsoft research-link quality source routing protocol (MR-LQSR) (5) etc. come under the category of reactive routing protocols.

Dynamic source routing (DSR)

- DSR is considered to be a very efficient routing protocol for wireless ad hoc networks. So many protocols have been derived from DSR to suit respective networking environments.

DSR is a widely used protocol for simulating, evaluating and testing new protocols, metrics and other networking characteristics. Dynamic source routing mechanism is divided into two stages.

- 1.Route Discovery: In this stage, Routerequest messages(RReq) originated from source 'S' are flooded across the entire network. Once the destination 'D' received any RReq message, it unicasts a Routereply(RRep) to the node from which it had received RReq packet. This RRep is eventually sent to source 'S' by spanning multiple hops. This way source gets a list of all possible routes to destination 'D' to choose from. A route is selected based on a better metric value. The metric used in plain DSR is hopcount. So, always the shortest paths are selected.

- 2.Route Maintenance: In this stage, source node checks if the established route between the source and the destination is working in case of any topology changes or attacks. A RouteError message is sent to the source when the route is found to be broken at some point. When such thing happens, source either uses a different route or starts route discovery again.

- There is no periodic update routing overhead in DSR and routing is fully ondemand.

Ad hoc ondemand distance vector routing (AODV)

- AODV routing protocol is another source routing protocol and is an improved version of DSDV.

- AODV find routes ondemand unlike DSDV that maintains routes to all destinations.

- **1.Path Discovery stage:** In this state, the source node sends Routerequest(RReq) to its neighbors which then forward the RReq to their neighbors and so on until the destination is reached or the node that have a fresh route to the destination is reached. RReq contains broadcastID which is incremented everytime a RReq is propagated over a different link, source sequence number,a fresh sequence number the source has it for the destination and destination's IP.

- Once RReq reaches the destination or the node that has a fresh route to the destination, the Routereply originated from the destination node or the intermediate node that has a fresh route to the destination is unicasted following the reverse route to the source. Every node stores each node's address from which they received RReq thus establishing a reverse path.

- **2.Route maintenance:** Every route is maintained along with a timer and when it expires the route is no longer used. Route maintenance is very similar to that of DSR.

Multi radio-Link quality source routing protocol (MR-LQSR)

- MR-LQSR is very similar to DSR except for the fact that MR-LQSR uses a link quality based metric called WCETT (Weighted cumulative expected transmission time) while DSR uses hopcount as its metric. Hopcount is not very suitable for wireless networks and more of this is covered in the next subsection.

2.1.2.3 Secure routing protocols

Secure routing protocols are another sect of routing protocols that have some security features attached to them. Authenticated Routing for Ad hoc Networks (ARAN) (15), Secure AODV (16)etc. are a few examples of secure routing protocols. Secure routing protocols employ a set of cryptographic certificates to provide security to the routing mechanism. Secure AODV routing protocol differs from AODV by having security extension packets for route requests, route replies and route errors. A brief description of ARAN is as follows.

Authenticated routing for Ad hoc networks

- ARAN provides security in terms of authentication, message integrity and nonrepudiation.

- ARAN routing mechanism is a four stage process. First stage is the certification stage, where a trusted third party server issues certificates to the nodes that are willing to enter the network. Then follows the authenticated route discovery stage where the source

and destination nodes are authenticated end to end by exchanging certain data. Route discovery stage is very similar to that of DSR except that it involves signature validation at every hop. The next stage is authenticated route setup where a route is established once the source verifies the destination correctly. Then comes the Route maintenance which is very similar to that of any ondemand routing protocol.

- ARAN is able to counter attack Unauthorized participation attack, spoofed route signaling, fabricated and altering routing messages, replay attacks etc but is not able to counter attack wormhole attack.

In short, Secure routing protocols provide security along with cryptographic overhead thus creating a certain imbalance between security and performance of the system. The proposed routing metric VBPQ in this thesis prevents a few of the packet dropping attacks without any need of cryptography and thus eliminating cryptographic overheads.

2.1.3 Routing metrics in wireless ad hoc networks

A lot of routing metrics have been designed for wireless ad hoc and mesh networks so far. Hopcount metric, ETX(4), ETT(5), WCETT(5), AETD(7), mETX(28), MIC(27) and iAWARE(30) etc.

- **Hopcount:** This metric is the most common metric used in wireless ad hoc networks. The routes with minimum hop count are selected. Hopcount metric is not suitable if the networking environment is wireless. The reasons are very simple. Hop count metric does not take quality of a wireless link, interference and radio patterns, data rate, packetsize etc into consideration. Hopcount does not even consider the effect of multiple radios in the network.

- **ETX:** This metric takes link quality into account. ETX is the expected number of transmissions (including retransmissions) required for a packet to be successfully transmitted over a wireless link. ETX takes forward and reverse loss rates of a wireless link into account and predicts the number of transmissions(including retransmissions). ETX is

additive in the sense that the ETX of a route is the sum of ETXs of links that constitute that route. The route with a low ETX value is selected. ETX does not take available bandwidth or packetsize into account.

$$ETX = 1/(d_f * d_r) \tag{2.1}$$

where d_f and d_r are the delivery ratios in forward and reverse directions respectively.

- **ETT:** ETT is the expected transmission time a packet might take to travel over a link. ETT is equal to the product of ETX calculated from the above equation and the estimated bandwidth B for a packet with size S.

$$ETT = ETX * S/B \tag{2.2}$$

In (5), B is estimated using packet pair technique (31). Using this technique, each node sends a small probe and a large probe back to back to its neighbor every minute. The receiver calculates the time difference between the reception of the two probes and sends this value to the sender. Then the sender calculates the bandwidth by dividing the size of the large probe with the minimum time difference calculated from atleast 10 samples. Like ETX, ETT also does not consider the effect of channel diversity and a route with lowest sum of ETTs of individual links is preferred.

- **WCETT:** WCETT is the weighted cumulative expected transmission time taken to send a packet from end to another end of the route. WCETT is a path metric for multi radio multi hop wireless ad hoc networks that takes the total ETT and the channel diversity into account. Channel diversity is calculated from the bottleneck ETTs which will be discussed clearly in the related work section. WCETT offers a trade off between throughput and delay. Route with lowest WCETT is selected.

- **AETD:** Adjusted expected transfer delay is an improvement over WCETT. AETD considers jitter alongside delay. Jitter is the time taken between consecutive packet trans-

missions. The authors of (7) introduced a new term called EDJ (expected delay jitter) to reflect actual channel diversity while claiming that WCETT does not actually reflect the channel diversity. More of this metric is discussed in later sections. Route with lowest AETD is selected.

- **mETX:** mETX is very similar to ETX except for the fact that mETX operate at bit level. Bit error probabilities are calculated by noting down the corrupted bits' positions ans their dependence over successful packet transmissions. This metric is a lot better to cope with link quality variations and to deal with medium instability.

- **MIC:** This is the metric that deals with interference and channel switching.

- **iAWARE:** iAWARE measures link quality variations by using signal to noise ratio (SNR) and signal to interference and noise ratio (SINR). iAWARE calculates the estimated busy time of a medium that has interfering nodes.

2.1.4 Attacks and countermeasures

Wireless networks are undoubtedly the replacement for wired networks. Each type of networks has their own advantages and disadvantages. One serious disadvantage of wireless networks is that they are more vulnerable to attacks than the wired networks. Wireless links can be eavesdropped or can be monitored just by staying in the range of transmission. Wireless ad hoc networks are much more vulnerable since they do not have any access point architecture to manage atleast some basic security issues like authentication etc while joining or leaving the network. Nodes work on mutual trust amongst them. Most of the attacks disrupt routing. In this section, a brief discussion on some of the attacks on routing and available countermeasures against those attacks is provided. This work's main contributions lie in the aspects of routing in wireless ad hoc networks. In the first part of this work, a possible DOS attack on routing which is termed as delay-variation attack is introduced. A possible countermeasure is also proposed by introducing a new routing metric for link quality source routing protocols. As part of the second contribution of this work, a countermeasure against wormhole attack which

when launched causes routing mechanism to misbehave is provided. The rest of this subsection discusses some of the earlier work related to the contributions of this work.

Routing attacks can be classified as two types. 1. Routing disruption attacks 2. Resource consumption attacks.

- **Routing disruption attacks:** In this type of attack, the routing mechanism is majorly affected. Attackers create routing loops that make control packets unreachable to the actual destinations. An attacker may also launch some fake control packets or forge them to detour the packets on a different route that may involve bad intent. Due to spoofed or altered messages, network may be partitioned or the routes may be shortened or extended or the link qualities may be deteriorated. These attacks are very serious attacks that may also lead to resource consumption attacks. Some of the examples of these attacks are blackhole attack, grayhole attack, gratituitous detour, rushing attacks, wormhole attack etc. The rest of this section talks about the attacks and some of the corresponding countermeasures.

  - **Black hole attack and Gray hole attack.:** In this attack, the attacker tries to attract packets by projecting a shortest route to the destination or a very good link quality. Attacker can launch this type of attack by removing some intermediate node addresses from the route request packets so that shorter routes are falsely projected. Gray hole attack drops only selected packets, not all.

    Countermeasures:

    * Ariadne routing protocol (17) employs a per hop hashing mechanism for authenticating each route request packet. This method uses cryptographic techniques like MACs etc to prevent this attack. However this involves a definite computation overhead because of cryptographic methods employed for every control packet.
    * In (23), to prevent these type of attacks, a data mining approach called Cross Feature analysis was proposed. Blackhole attack was launched by generating

bogus route requests that had maximum allowed sequence numbers in them so that the routes always appear fresh. More of this cross feature analysis is discussed in further sections.

- **Rushing attack** Rushing attack is said to be launched when duplicate control packets are suppressed at the destination. The attacker spreads control packets very quickly so that the nodes would reject the duplicate and legitimate packets later. The rushed control packets in general allow the old valid routes to be replaced by the routes that involve the attacker. A more serious rushing attack may as well lead to wormhole attacks.

  Countermeasure:

  * (18) proposed a prevention mechanism against rushing attacks especially for on demand routing protocols. This mechanism is an add-on to route discovery mechanism and is called as Rushing Attack Prevention (RAP). RAP is implemented in steps. First step is called secure neighbor detection where both the sender and receiver check each other if they are in the wireless transmission range. Second step is secure route delegation where both the sender and receiver of a route request believe that they are indeed neighbors. Third step involves randomized forwarding in which a node collects a certain number of requests and then forward a request selected randomly from the list. Then follows the secure route discovery basing on the fact that the legitimate node generates only one legitimate route request.

- **Wormhole attack:** Wormhole attack is one of the most difficult attacks to prevent or detect. When wormhole attack is launched, two distantly located nodes think that they are neighbors but in fact they are not. This is possible when two colluding attackers, each located close to the affected nodes, are connected via a high speed tunnel and the signals from one end are replayed to other end through this high speed tunnel. High speed tunnel can be anything like a low latency wired connection, high power wireless link etc. This attack especially disrupts the routing behavior

and is able to source node to always select a route that involves this wormhole. The reason is very simple. Since two distantly connected nodes are connected via a virtual tunnel, they appear closer. So, the routes involving wormhole attack will be of length one or two. There have been many countermeasures mentioned for wormhole attack prevention and detection. Figure 2.1 shows the wormhole attack caused by two outsiders(colluding attackers).

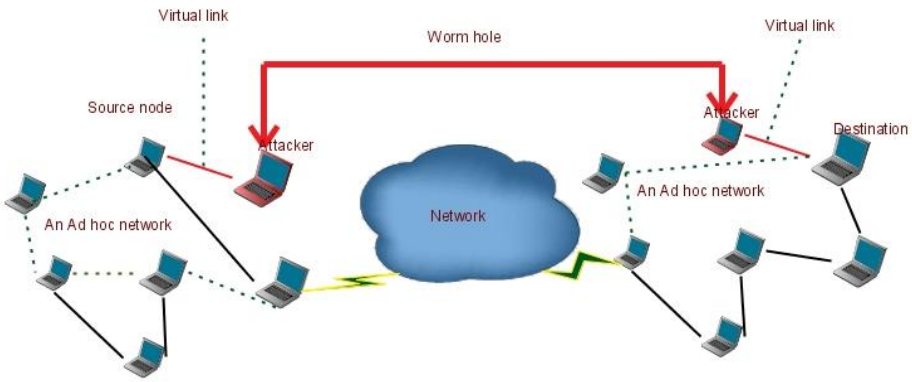


Figure 2.1 **Wormhole attack**

The above figure 2.1 shows an ad hoc network constituting two small networks interconnected. The green dotted lines show the actual and valid route available from the source to the destination which is several hops away from the source. The attackers shown in red are the outsiders whose presence is unknown to the nodes in the ad hoc network. The route shown in red is the attackers route. The thick line shown there is a wormhole that tunnels the copied signals at both the ends. There have been many countermeasures designed to prevent and detect wormhole attacks.

Countermeasures:

* **Packet leashes:** Packet leashes is a technique employed in (19) to detect wormhole attack. A packet leash is a piece of information that put brakes on the packet's maximum allowed transmission distance. This is the definition taken from (19). Packet leashes are of two types, 1. Geographical leashes and 2. Temporal leashes. In geographical leashes, each node is loosely synchronized

with one another and knows its location information. A geographical leash guarantees that the receiver is with in certain estimated distance from the sender. A temporal leash estimates a bound on the life time of the packet which inturn restricts the maximum allowable distance between the nodes.

  * **LITEWORP:** LITEWORP is more suitable to resource constrained networks like wireless sensor networks. It uses two stages to detect the nodes that are involved in wormhole attack. The first stage is a two hop neighbor discovery stage where the neighbors who are two hops away. Second hop neighbor information is used to determine if a packet is legitimate or not. For example, say suppose a node C receives a packet forwarded by a node B intended to come from a previous hop node A, then C could discard the packet if A is not its second hop neighbor. After the two hop neighbors and one hop neighbors are discovered, node locally monitors traffic going through its neighbors and becomes a guard while satisfying some security assumptions provided in the paper (20). The authors of the paper have also provided an algorithm that detects the nodes that involve in launching wormhole attack.
  * (22) provides another way to detect the endpoints that cause the wormhole. The authors of this paper have proposed an algorithm called EDWA (end to end detection of wormhole attack) that estimates the hop number using some geographical information at the source node. If the estimated hop number is greater than the actual hop number in the packet, then an alert of wormhole attack is generated. After the hidden wormhole attack is detected, the authors have proposed a TRACING algorithm that detects the end points of the wormhole.

- **Resource consumption attacks** Valuable network resources like bandwidth, nodess memory and storage power are targeted. Injecting extra data packets into the network is an example of Resource consumption attack.

2.1.5 Datamining techniques: Detecting routing anamolies

Though Datamining is a very recent term introduced in 1990s, its roots are relatively older. Statistics can be considered as the foundation for the evolution of data mining techniques. With the increase in computing power and due to a rapid technological advancements oflate, the field of artificial intelligence has been advancing at a greater speed too. Artificial intelligence, a relatively old term is definitely a major contributor towards datamining and its evolution. A mix of statistics and artificial intelligence paved way to a nicer discipline called Machine learning. Many efficient machine learning algorithms have been designed till date to mine huge chunks of data. In this thesis, a popular routing anamoly called wormhole attack is detected by employing a machine learning algorithm proposed in (23). Datamining refers to the process of discovering data of interest from huge databases. The size of the databases is increasing everyday and datamining algorithms are more fine tuned and enhanced to be more efficient to analyze the data of interest in a real quick time. A lot of information on data mining is found in (Data mine)

Datamining finds its applications mainly in the fields of Bio-informatics, banking, intrusion detection systems etc. In this thesis, data mining is used in detecting a routing anamoly. There has been quite a lot of research going on in this area of detecting anamolies or intrusions. One of the most important applications of datamining is classification. Classification is the process of predicting a class for a particular data entry based on some rules. Rule based induction, decision trees etc are some of the approaches of classification. In general, a classification model is built based on some available training data set. Test data is fed to this system and each data entry is assigned a class based on the classification rules. In (23) authors have proposed a new data mining technique called cross feature analysis for detecting routing anamolies in wireless ad hoc networks. Due to, cross feature analysis technique, the authors of (23) were able to find correlations amongst the features in normal traffic. More of this discussed in the next subsection, that is related work.

Datamining algorithms are developed based on what kind of data mining task is required. Data mining tasks can be classified as classification, clustering methods, feature selection,

regression etc. Clustering techniques are extensively used in pattern recognition systems, Bio-informatics, natural language processing etc. Clustering is effectively used for data storage reduction where the entire data set is clustered into a few groups and each group is headed by a clusterhead. So the nodes that belong to a particular group can be represented by a clusterhead. This way, clustering is one way of analyzing the data by grouping data entries together to convey some useful information. Data items are grouped basing on some distance measure. Eucledian distance measure is a very simple example of measuring the distance between two data objects employed in kmeans clustering technique (32). Clustering has also its applications in anamoly detection. In (33), the authors have come up with a learning approach that takes temporal sequences of discrete data to characterize the networks. Discrete data include command traces, GUI events, network traffic etc. They employed instance based learning(IBL) technique and came up with a distance measure that suits the temporal sequences of discrete data.

2.2 Related Work:

2.2.1 Related work: VBPQ

In (5), the authors have proposed a routing metric called WCETT (Weighted Cumulative Expected Transmission Time).These authors have used this metric in a routing protocol called Multi-radio Link quality Source routing protocol (MR-LQSR) which was implemented in their mesh network toolkit. WCETT takes link quality and channel diversity into account. The authors in (5) measured link quality in terms of Expected transmission time (ETT). Calculation of ETT requires the forward and reverse loss rates and also the available bandwidth of the link.

$$ETT = ETX * S/B \tag{2.3}$$

where ETX is Expected transmission count proposed in (4) that takes forward and reverse loss rates of a wireless link into account and predicts the number of transmissions(including retransmissions), S is the packet length and B is the bandwidth of the link.

$$WCETT = (1-\beta) * \underbrace{\sum_{i=1}^{n} ETT_i}_{TETT} + \beta * \underbrace{max_{1 \leq j \leq k} X_j}_{BETT-channeldiversity} \tag{2.4}$$

where X_j is the sum of the ETTs of the links on channel j, n is the total number of hops and k the number of channels. Second term in the equation 2 indicates ETT of the bottleneck channel. β is the tuning parameter.

This metric was designed especially for multi radio multi hop networks. With multiple radios on each node, the capacity of the networks is increased as two radios can transmit and receive simultaneously on orthogonal channels. Otherwise, the capacity is halved with only one radio per node. The authors of (5) have assumed that the radios are tuned to non-interfering channels by some outside agency. One can view this WCETT metric as the trade off between the end-to-end delay of a route (TETT) and the throughput (Bottleneck ETT) of that route. The authors of (5) did not consider the impact of interference caused by nearby nodes and also the differential interference which makes low bandwidth link more preferable to high bandwidth ones. The readers are recommended to go through the details of (5) to know better about the metric.

But the problem with WCETT metric is that it may not reflect the actual channel diversity as claimed by (7). WCETT may not account for simultaneous transfers on the links that lie in the same interference region. The authors of (7) proposed a new metric called AETD (Adjusted expected transfer delay) that replaces BETT in equation 2 with EDJ (Expected delay jitter between consecutive packet transmissions), that might as well reflect the actual level of channel diversity. The EDJ formula is a recursive formula that takes the interference range in terms of hops, into account. The formula of AETD is as follows.

$$AETD = (1-\alpha) * \underbrace{\sum_{i=1}^{n} EDT_i}_{TETT} + \alpha * EDJ \tag{2.5}$$

EDJ is calculated recursively as follows

$$EDJ_{r(i)} = \begin{cases} ETT_{h_k}, & \text{if } i = k-1; \\ ETT_{h_{i+1}} + EDJ_{r(i+1)}, & \text{if } \exists i+1 < j \leq min(i+m+1, k); \\ , & \text{such that } C_{h_{i+1}} = C_{h_j} \\ max(ETT_{h_{i+1}}, EDJ_{r(i+1)}), & \text{otherwise.} \end{cases}$$

where α is again the tuning parameter ranging between 0 and 1. Small $'\alpha'$ leads to a route that is less zigzag.

The authors of (7) illustrated with an example and showed that their metric AETD selects more channel diverse paths when compared to those selected by WCETT. As can be observed from (4)(5)(7), AEDT is more performant than WCETT, ETX, HOP in multi radio multi hop networks especially when there is an increase in the number of channels, node density etc. This study shows that the metric VBPQ will be able to select paths that are more reliable than that can be selected by AETD or WCETT. Here, reliability is defined based on a simple intuition that is "Higher the ETT of a packet on a link, less is the reliablity that the packet is transmitted or received over that link." This way, any routing protocol that incorporates VBPQ tends to be highly robust which is what we require for a wireless mesh network to provide reliable service. In this process of providing reliability, we are not incurring any security overhead while still ensuring security against some of the packet dropping attacks. In the subsequent sections, we will be providing our metric and the discussions related to it.

2.2.2 Related work: WHDetect

One of the most important contributions of this thesis is to propose an algorithm (WHDetect) for wormhole attack detection for wireless ad hoc networks. The detection process involves a machine learning technique proposed in (23). In (23), the authors were able to detect network anamolies like black hole attack, update storms, and packet dropping attacks. The machine learning technique implemented in (23) belongs to the realm of feature attraction mining tasks and is termed as cross feature analysis. Cross feature analysis basically deals with the corre-

lations amongst features. Features may include type of control packets, sampling time, link quality ETT, packetsize etc. Cross feature analysis is set to solve a classification problem $f_1, f_2, f_3, ..., f_{i-1}, f_{i+1}, ...f_m -> f_i$ where $f_1, ..., f_m$ is a feature vector and m is the number of features. The steps for solving this problem is as follows:

- First of all, a training data model is constructed from the normal data. It is assumed that atleast one feature from the feature set should be able to distinguish from the normal and abnormal events.

- Next, the submodels are built by selecting each feature as a target feature. Each submodel predicts the class for the corresponding target feature. Generally, predicted classes for normal events are same as their true classes but the predicted classes for abnormal events may not be same as their true classes. If so, then the anamolies are detected other wise they go in the list of false positives or false negatives or false alarms.

- The system of submodels is called the detection system. First the training set is fed to this detection system. There are many ways to actually classify the events like count method, probability method, RIPPER etc. Submodels are basically trained in this step. After the submodels are trained, a decision threshold is formulated. The decision threshold depends completely on the working environment. In general, minimum count or minimum probability can be taken as thresholds. Predicting a class of a new event is discussed in the next chapter.

- In the next step, anamolous data is fed into these submodels and appropriate classes are assigned to each anamolous feature vector. The classes are assigned based on the underlying decision threshold.

Threshold selection

The selection of a threshold is very critical in classifying whether a data object is normal or abnormal. Improper selection of threshold will result into false alarms which is undesirable. In (23), there are quite a few threshold detection techniques mentioned. Of them, Count method and probability method are the ones that are considered in this thesis.

- **Count method**: First, the normal data is fed into the detection system and each data entry is assigned a counter value which is incremented as and when this is observed in any submodel. This counter value is normalized by dividing it with the number of features. Now threshold can be selected as the minimum of all the normalized counters assigned to every normal object.

- **Probability method**: In this method also, first the normal data is checked through submodels and this time each data entry is assigned a probability. Count method is a binary method (0 for a mishit, 1 for a hit in the submodel) where as probability method assigns probabilities that range from 0 to 1. Threshold value is equal to the minimum of all the probability values.

CHAPTER 3 PROPOSED METHODS

The first part of this chapter discusses the newly proposed metric VBPQ as to how VBPQ counter attacks a possible attack that can disrupt routing. In the second part, an algorithm WHDETECT that can detect wormhole attacks in link quality based routing protocol is mentioned.

3.1 Proposed Metric: VBPQ

In this study, VBPQ is formulated in two different ways. First variant of the metric is basically an extension to WCETT or AETD. Second variant of the metric and the motivation behind formulating it is discussed in the 'Discussion' section. The next subsection talks about the assumptions that this chapter makes before formulating the metric VBPQ.

3.1.1 Assumptions

- **Network model:** The network model under consideration is any wireless ad hoc network where the nodes in the network are fixed. Wireless mesh backbone network is an able fit to this model. Mesh backbone network is especially considered because the metric VBPQ is able to meet some design issues of wireless mesh networks in terms of connectivity, security and reliability.

- Every node is employed with more than one radio. The radios may be all 802.11a or all 802.11b or all 802.11g or a mix of these. In the experiments, only 802.11b radios have been mounted on every node.

- There is no limit on the number of radios on each node.

- The radio on a particular node is tuned to a particular channel at any particular time.
- If two adjacent links are on the same channel, they are said to interfere with one another.
- When two adjacent links are on two different channels they are assumed to be non interfering with each other. And channels from two different radios are non-interfering.
- In (5), the authors assumed that packet lossrate is an independent parameter and the same holds here in the derivation of VBPQ.
- ETTs on forward and reverse links need not be same as ETT is an asymmetric link quality metric.
- If AETD metric is used as the submetric in the formulation of VBPQ, then hopbased interference is assumed as mentioned in (7).
- **Attackers model:** The attackers in the model are basically insiders. They work in tandem to produce a type of denial of service attack called as delay-variation attack. They can turn a good link into a bad one by inducing some congestion on to the link. The attackers are considered to be atleast as powerful as a normal node in the network.
- **Security assumptions:** A minimal security policy that maintains message integrity, data confidentiality, authentication and non-repudiation is a prerequisite. Especially, no node can tamper the integrity of a message. Even if tampered, it is assumed that the actual message is recovered using some integrity preserving cryptographic techniques.

3.1.2 Metric: VBPQ

VBPQ is devised based upon the following definition which has been taken from a simple intuition taken from ETX (4) and ETT (5) that is higher the ETT or ETX lesser is the quality and reliability of the link .

Relative reliability: Link 'i' is relatively reliable to link 'j' iff $ETT_i < ETT_j$. To capture this simple intuition, a new term variance is introduced as part of VBPQ which acts like a reliablity indicator of the entire route.

Following are the terms and definitions used in the formulation of VBPQ.

Average ETT of a route where n is the number of links of that route:

$$AETT = (\sum_{i=1}^{n} ETT_i) \div n \tag{3.1}$$

It is possible that more than one route may have the same ETT value or may have the same WCETT or AETD value. In that case, it is very hard for the source node to determine which one is the best route to select. In the example provided later in this section, it is shown that VBPQ metric differentiates such kind of routes which AETD or WCETT cannot differentiate. Variance based path quality routing metric actually favors the paths that have less deviation from the Average ETT value of entire path. This implies that the paths that are selected using this metric are not as lossy as the paths that are selected using the metrics WCETT or ADET and therefore providing reliable and robust routing.

Deviation and Variance of a path, where n is the number of links of that route:

$$\begin{aligned} DETT &= (\sum_{i=1}^{n}((ETT_i - AETT)^2)) \\ VETT &= DETT \div n \end{aligned} \tag{3.2}$$

VBPQ presented below can be viewed as the balance between the performance of either WCETT or AETD and the reliability of the route. In VBPQ, VETT measures reliability.

$$VBPQ = (1-\gamma) * (AETDorWCETT) + \gamma * VETT \tag{3.3}$$

If WCETT is used as the sub metric:

$$VBPQ = (1-\gamma) * ((1-\beta) * TETT + \beta * BETT) + \gamma * VETT \tag{3.4}$$

If AETD is used as the sub metric:

$$VBPQ = (1-\gamma) * ((1-\alpha) * TETT + \alpha * EDJ) + \gamma * VETT \tag{3.5}$$

where γ is the tuning parameter ranging between 0 and 1(not including 1). Setting $\gamma = 0$ implies that the routes that are selected by VBPQ are same as the ones selected by AETD or WCETT. As γ increases, the reliability increases in the network. But when γ reaches one, there will be no more channel diversity. Therefore, setting γ to 0.5 must give a perfect balance between the two terms in the metric. The values of α and β can be set according to the values suggested by the authors of (7) and (5) respectively.

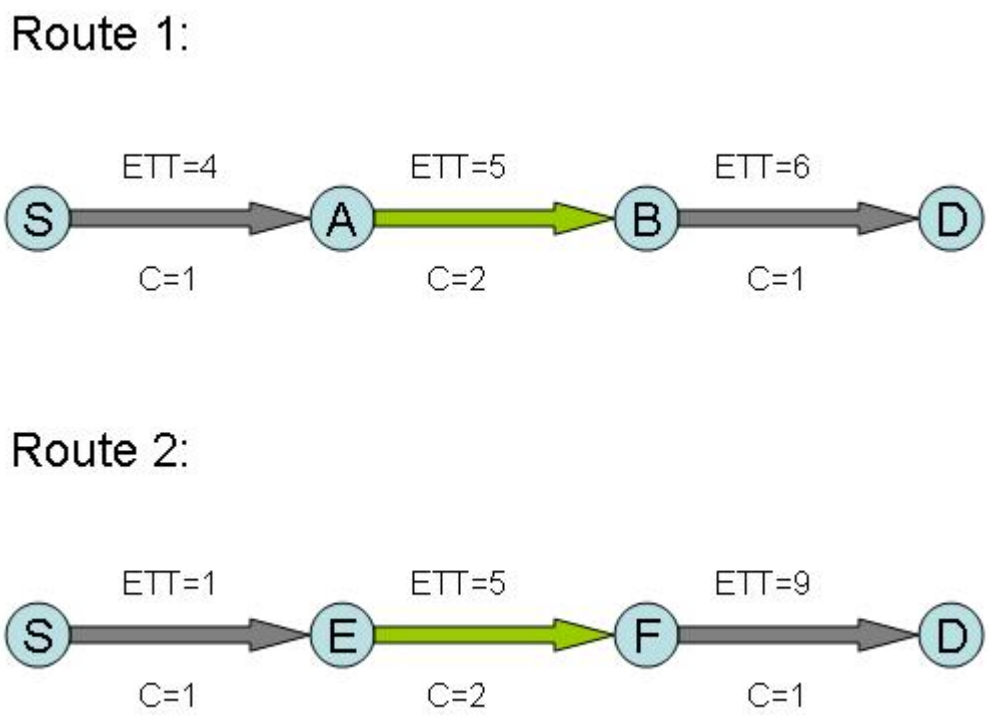


Figure 3.1 **Example: Route selections of AETD, WCETT and VBPQ.**

This figure shows two possible routes from source S to destination D. ETTs of each link are indicated on top of each link. Channel numbers are seen at the bottom of each link. Grey color indicates that the link is on channel 1 and green indicates that the link is on channel 2. Variance of route 1 = 2/3, Variance of route 2 = 32/3.

Table 3.1 **Route Selections by AETD, WCETT and VBPQ**

Routes	WCETT (col1)	AETD (col2)	VBPQ	
			WCETT	AETD
route1	$(1-\beta).15+\beta.10$	$(1-\alpha).15+\alpha.10$	$(1-\gamma).(col1)+\gamma.2/3$	$(1-\gamma).(col2)+\gamma.2/3$
route2	$(1-\beta).15+\beta.10$	$(1-\alpha).15+\alpha.10$	$(1-\gamma).(col1)+\gamma.32/3$	$(1-\gamma).(col2)+\gamma.32/3$

3.1.3 An Example

A simple example is provided to illustrate the route selection made by VBPQ. Figure 3.1 shows two routes taken from an arbitrary network topology and the text above and below each arrow represents ETT and channel number respectively. As one can observe that from both the routes, channel 1 is the bottleneck channel.

As can be observed from Table 1, neither WCETT not AETD is able to differentiate two routes where as metric VBPQ is able to differentiate one route from another and selects Route 1 since there is probability that more packets are dropped on route 1 when compared to that on route 2. As can be observed from Figure 3.1, Bottleneck ETTS and EDJs for both the routes are equal. Hence, it is evident that the values of WCETT, AETD are equal for both the routes. Selecting route 2 is not a good idea since $ETT_{FD} = 9$ is greater than $ETT_{BD} = 6$ and has link FD has more chance of dropping packets than that of link BD. Therefore route 2 is not reliable as route 1 though TETT is same for both the routes. Reliability might even decrease when networks scale. With VBPQ, route 1 is selected since the variance of route 1 is less than that of route 2 and hence selects a reliable and attack free route.

3.1.4 Attack Scenario

This kind of selection can be viewed as a different way that offers some security to the routing protocol. An attacker can always manipulate or fake the ETT values or can intentionally increase the retransmissions or can drop the packets by keeping the TETT of the route unchangeable. This way, the attacker is able to induce denial of service attacks into the network. This type of attack is from now called as Delay-Variation attack. It can be considered as a variant of Gray-Hole attack (Attracting and Selectively dropping the packets) and also

a colluding attack caused by the insiders. This is where metric VBPQ comes handy when compared to AETD or WCETT. If at all, an attacker fakes a higher ETT value on some link keeping the TETT of that route same the variance of that route is inevitably increased which allows the source to avoid this route and select the route that is better in terms of VETT.
In the Results section, it is shown that VBPQ outperforms WCETT, AETD and ETX when under this kind of attack. So, VBPQ provides security and reliability in routing without incurring any cryptographic overhead and without hindering any performance.

3.1.5 Discussion

In this section, the motivation behind formulating our metric in a different way is provided. In the following example, an inherent problem while calculating WCETT and AETD is discussed. The problem comes when we take the weighted average between TETT and the respective channel diversity term. For example, in 3.1, take route 1 for instance.

$$\begin{aligned} TETT &= 4+5+6=15 \\ BETT &= 4+6=10 \\ EDJ &= 4+max(5,6)=10 \end{aligned} \tag{3.6}$$

$$\begin{aligned} AETD &= (1-\alpha)(4+5+6)+((\alpha) \\ &\quad *(4+max(5,6))) \\ &= 15-(5*\alpha)+((\alpha)*(4+6))-((\alpha) \\ &\quad *(4+6)) \\ &= 15-(5*\alpha) \\ WCETT &= (1-\beta)(4+5+6)+((\beta)*(4+6))) \\ &= 15-(5*\beta)+((\beta)*(4+6))-((\beta) \\ &\quad *(4+6)) \\ &= 15-(5*\beta) \end{aligned} \tag{3.7}$$

From the above derivations, one can observe that the channel diversity term in both the calculations of AETD and WCETT cancels out when the first term is expanded. In effect, the metrics AETD and WCETT are not leveraging the effect of channel diversity at all or may be the metrics are not very straightforward in their formulation. To leverage the effect of channel diversity in a more straightforward way, a different variant of VBPQ metric is proposed.

If WCETT is used as the sub metric:

$$\begin{aligned} VBPQ &= (1-\beta)*(\underbrace{((1-\gamma)*TETT+\gamma*VETT)}_{ETTeffect} \\ &\quad +\beta*BETT \end{aligned} \tag{3.8}$$

If AETD is used as the sub metric:

$$\begin{aligned} VBPQ &= (1-\alpha)*(\underbrace{((1-\gamma)*TETT+\gamma*VETT)}_{ETTeffect} \\ &\quad +\alpha*EDJ \end{aligned} \tag{3.9}$$

From the above equations, one can see that the above equations create a perfect balance between the effect of ETT on the entire path and the effect of channel diversity. The term

'ETT effect' conveys the tradeoff that exists between packet dropping rate and reliablity of the route. Ideally speaking, γ must be set to 1. But while a packet is traversed along a path to reach the destination, it consumes some resources and takes some time. That expected time is measured by TETT. To reflect this, γ here is used as a tuning parameter that ranges between 0 and 1 that creates a balance between reliability and the end-to-end delay of a packet. α and β are the tuning parameters of AETD and WCETT mentioned in (7) and (5) respectively. This metric is not an enhancement over WCETT or AETD, it is totally a different metric that actually provides a tradeoff between end-to-end delay and the channel diversity of a route. EDJ is preferred to BETT here as it reflects channel diversity better than BETT.
In the results and analysis section, a few graphs explain the importance of our metric. We also show the effect of γ along with α and β respectively.

3.2 WHDetect: Algorithm to detect Worm hole attack

Wormhole attack is one of the most difficult attacks to prevent or detect. When wormhole attack is launched, two distantly located nodes think that they are neighbors but infact they are not. This is possible when two colluding attackers, each located close to the affected nodes, are connected via a high speed tunnel and the signals from one end are replayed to other end through this high speed tunnel. High speed tunnel can be anything like a low latency wired connection, high power wireless link etc. This attack especially disrupts the routing behavior and allows the source node to always select a route that involves this wormhole. The reason is very simple. Since two distantly connected nodes are connected via a virtual tunnel, they appear closer. So, the routes involving wormhole attack will be of length one or two. In general, a hopcount based soruce routing protocols are employed like DSR in wireless ad hoc networks. If that is the case, then shortest routes are selected and always the routes that involve wormhole attack are preferred and selected eventually. There have been many detection and prevention techniques discussed in the literature (19) (21)(20)(22). But none of them has talked about what if wormhole attack is caused in link quality based source routing protocols where hop count metric is not used as the routing metric. Wormhole attack is mainly caused

in route discovery stage. The tunnel acts like a magnet that attracts all the data once the route involving the tunnel is selected.

3.2.1 Assumptions:

- **Threat model:** In link quality source routing protocols there is no hopcount metric involved in route selection. So better quality routes are preferred to shorter routes that are suboptimal. How the attackers are able to launch the attack is the point of question is here. The attackers replay the control messages that involve ETT from end to the other end so that the end nodes become neighbors. The tunnel here shortens the route but may not attract the packets as link quality based routing protocols do not take hopcount into account. Attackers are virtual nodes. No node is able to detect the attacker. They eavesdrop on to the wireless links. Attackers have to be very intelligent in launching the wormhole attack. They have to select end nodes that possess very good link qualities to their neighbors. Otherwise, the tunnel cannot just attract the packets. This study assumes that the attackers cannot be any valid neighbors. The reason is very simple. If they are neighbors, they need not replay any signals from one end to other but they just have to forward the packets over the tunnel that almost has a ETT value of 0. This route adds upto the list of better routes from which the source may select any route. Since the attackers have compromised the nodes, they will not follow WHDetect algorithm that detects wormhole attack between those two. So in this case, it is very difficult to find wormhole attack. That is why, the attackers are assumed to be outsiders not seen to any of the insider nodes.

- The network model may be anything like a wireless ad hoc network.

- The wireless links need not be bi directional. It is left to routing protocol semantics.

- Every legitimate node is supposed to run this WHDetect algorithm to detect wormhole attack every time they receive a route reply.

- Every route reply packet is said to have location information of the node that originates it.
- Every route reply packet is set to contain the information regarding the features chosen for the cross feature analysis model.
- Every node also maintains ETT profile that looks like this. The profile shown below is just for the example sake.

Distance	Packetsize	Datarate	ETT
DIS1	PS1	DT1	ETT1
DIS1	PS2	DT2	ETT1
DIS1	PS2	DT3	ETT2
DIS1	PS2	DT2	ETT2

Table 3.2 **ETT profile**

3.2.2 Algorithm: WHDetect

- **Step1:** Whenever a node receives a route reply packet from its neighbor, get the location information, ETT value, datarate, packetsize etc.
- **Step2:** Calculate the actual distance between these two nodes from the location information available.
- **Step3:** Construct a feature vector that matches the underlying ETT profile, from the information available from the route reply packet.
- **Step4:** If (actual distance > transmission range of a node)

  Then Report "'Wormhole attack."'
- **Step5:** Else
  - Construct the detection subsystem from the ETT profile using cross feature analysis presented in (23)
  - set the threshold mechanism for anamoly detection to be probability method

* Feed the feature vector into the detection subsystem to predict the class of the route reply packet.
* If the class reports anamoly:

  Then Report "'Wormhole attack."'

  Else

  Categorize it as "'Normal packet"'

Algorithm description:

Every node in the network runs this algorithm whenever it receives a route reply packet. In general, route reply packets are unicasted while route request packets are broadcasted. So it is better to check for wormhole when a node receives route reply not when every time a route request packet is sent. This reduces a lot of computation overhead. Nodes have to agree upon the number of features. Of which, distance and ETT are one of the very important features and must be features for the wormhole attack detection. Actually one may argue why this algorithm employs cross feature analysis to predict the attack. One may write a simple algorithm that may not involve data mining at all very similar to the one proposed in (22), which is as follows.

Simple WHDetect

– If the 'Actual distance' > 'Max distance'

  Then straightaway conclude Worm hole attack. Else

  * Estimate the ETT value from the profile data base corresponding to the 'Actual Distance'
  * Take the minimum of ETTs corresponding to the actual distance.
  * If 'Actual ETT' < 'Min ETT'

    Then conclude Wormhole attack.

    Else

    False negative or may not be a Wormhole attack.

The above algorithm works very similar to the algorithm mentioned in (22). The above algorithm estimates the link quality instead of hopcount. But this algorithm just takes care of ETT and distance but does not account for other things like datarate, packetsize, sampling times etc. The correlation amongst these features are very important as they account for the calculation of link quality. Moreover, just comparing the actual ETT with MinETT is not enough for the purpose of anamoly classification. A proper data mining application has to be in place to measure the correlations amongst features and to classify normal data from abnormal data. That is why, a cross feature analysis mentioned in (23) is employed in WHDetect.

The complexity of WHDetect is nothing but the complexity of construction of the detection subsytem. Other comparisons can be done in O(1) time.

CHAPTER 4 RESULTS

Having discussed about the proposed metrics and algorithms to detect various attacks and countermeasures, it is now time to see the experimentation results and plots as to how the above contributions have met the problem statements of this thesis. This chapter is divided into two sections. First section portrays the experimentation results on the evaluation, performance and significance of Variance based path quality metric. This section introduces a new evaluation metric called 'Power of a route' along side already well known metrics like throughput, delay and jitter. Taking these evaluation metrics into consideration, metric VBPQ is compared with other link quality based metrics like ETX, WCETT and AETD. ETX is compared with VBPQ under single radio scenario where as WCETT and AETD are compared under multi-radio scenario. The second section shows recall-precision graphs for the two methods namely probability and count methods by varying thresholds. It will be shown that the probability method outperforms count method at all thresholds there by providing a better solution to detect wormhole attacks.

4.1 Results: Evaluation of VBPQ

In this section, various plots reflect the role played by VETT in the metric VBPQ. The plots are shown for both the variants of the metric. In the plots, x and y axes refer to the tuning parameters $\alpha(\beta)$ and γ respectively.

As an example, plots take the data from figure 3.1. In the following two subsections variant 1 and 2 of the metric VBPQ are discussed and plotted with respect to the tuning parameters $\alpha(\beta)$ and γ respectively. In the later sub-sections, simulation results to measure the performance of VBPQ are mentioned.

It is important to understand how at all values the statement "'lower the variance of the path lesser is the metric value by keeping the TETT, BETT or EDJ constant"' is true. Shown below is the mathematical analysis to prove that the above statement is right. It is clearly understood that the routes with the least metric value are selected. Simulation results in the later sections confirm to the mathematical analysis shown below.

Assume

$$VETT_1 < VETT_2$$

we know that

α,β, γ, TETT, BETT or EDJ, WCETT or AETD, and

also the VETTs are all positive

now,

$$\Leftrightarrow \gamma * VETT_1 < \gamma * VETT_2$$

$$\Leftrightarrow (1-\gamma) * WCETT(AETD) + \gamma * VETT_1$$

$$< (1-\gamma) * WCETT(AETD) + \gamma * VETT_2$$

$$\Leftrightarrow f_1 < f_2$$

4.1.1 Effect of $\alpha(\beta)$ and γ on variant 1

From figure 3.1, routes 1 and 2 can be represented as metric equations shown below. Here if WCETT is used as the submetric β is used as the tuning parameter and if AETD is used α is used as the tuning parameter. Since the values of EDJ, BETT and also TETT are equal, same set of equations for AETD and WCETT are obtained. Here let α=β.

Figure 4.1 shows a plot where dotted lines represent f_1 and the numbers on those lines represent the values of f_1 for various values of γ and β. Bold lines represent f_2 and its values. As is clearly evident from the figure 2, f_1 is always lesser than f_2. Routing protocol is meant to select the value that has the least value, and in this case it is f_1. Therefore route 1 is preferred

to route 2. As can be observed from the following functions, As VETT value is increased, the function value is also increased. This implies that VBPQ metric finds a more reliable path correctly based on VETT values.

$$f_1 = (1-\gamma) * ((1-\beta) * 15 + \beta * 10) + \gamma * 2/3$$

$$f_2 = (1-\gamma) * ((1-\beta) * 15 + \beta * 10) + \gamma * 32/3$$

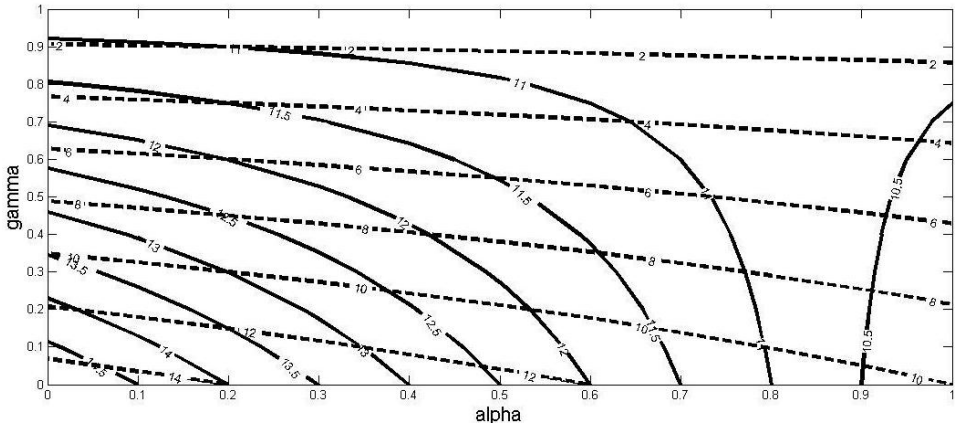


Figure 4.1 **Effect of $\alpha(\beta)$ and γ on variant 1**

Dotted Lines represent f1 and Bold lines represent f2. The values on top of the lines represent the values for f1 and f2 when the tuning parameters are changed accordingly. X-axis represents the tuning parameter employed in WCETT or AETD and Y-Axis represents the tuning parameter for VBPQ. Both the axes scale from 0 to 1. f1 and f2 represent route1 and route2 respectively.

4.1.2 Effect of $\alpha(\beta)$ and γ on variant 2

For variant 2, the equations are changed a bit accordingly. The same old routes are taken from figure 1. Figure 4.2 shows the plot for variant 2 of VBPQ. Here are the following equations.

$$f_1 = (1-\gamma) * ((1-\beta) * 15 + \gamma * 2/3) + \beta * 10$$

$$f_2 = (1-\gamma) * ((1-\beta) * 15 + \gamma * 32/3) + \beta * 10$$

Here to address the issue of channel diversity, these equations are formulated. Here γ acts as the tradeoff paramter between reliability and channel diversity of a route. Figure 4.2 shows the effect of both the tuning parameters on the metric. As can be observed from the figure 4.2, f_1 always gives us the least value for all values of γ and β. Dotted lines represent f_1 and bold lines represent f_2. So, VBPQ is able to differentiate the routes with VETT or DETT value. This also suggests that even using second variant of the metric, the metric is able to find reliable routes correctly.

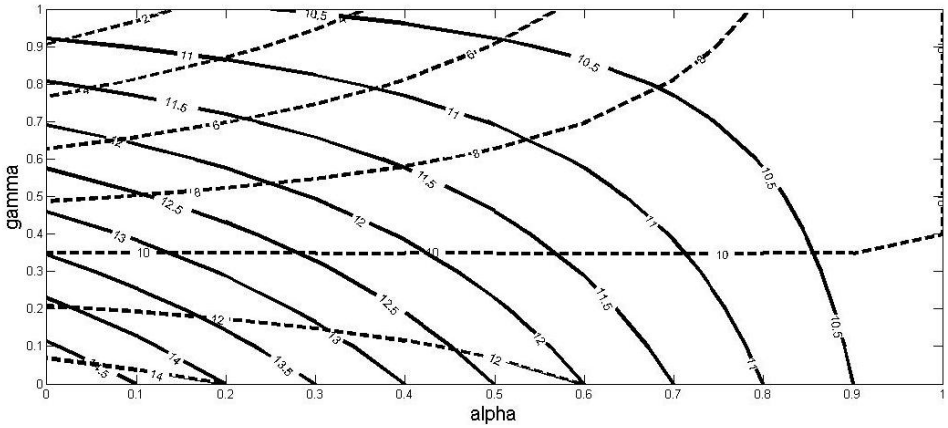


Figure 4.2 **Effect of $\alpha(\beta)$ and γ on variant 2**

Dotted Lines represent f1 and Bold lines represent f2. The values on top of the lines represent the values for f1 and f2 when the tuning parameters are changed accordingly. X-axis represents the tuning parameter employed in WCETT or AETD and Y-Axis represents the tuning parameter for VBPQ. Both the axes scale from 0 to 1. f1 and f2 represent route1 and route2 respectively.

4.1.3 Performance Evaluation

In this sub-section we show the performance evaluation of metric VBPQ using Qualnet Simulator(Qualnet). The performance comparison of various metrics when the attack is on is also shown and discussed in detail.

4.1.3.1 Simulation setup: Qualnet

The Simulation setup is carried out in a square flat area with dimensions $1500m \times 1500m$, where each node is employed with 1-4 radio interfaces depending upon the type of experiment. The simulated network is a static network very similar to a mesh backbone network. Two different types of experiments are carried out on this simulation setup. One is single radio experiment where each node is employed with only one radio and the other, multi-radio experiment, where the nodes are employed with more than one radio interfaces. Each radio interface is of type IEEE 802.11b (802.11b). Since WCETT has no problems with having a mix of 802.11a,b, and g radios and VBPQ is basically an extension to WCETT, it is assumed that VBPQ works fine with mix of 802.11 a,b and g radios. All tests are carried using only 802.11 b radios for simplicity. Each radio interface is able to operate at any one of the available data transmission rates namely 11 Mbps, 5.5 Mbps, 2Mbps and 1Mbps. The corresponding transmission ranges are 304m, 360m, 390m, and 500m respectively. A fixed data rate of 11Mbps is followed in all of our experiments except in some special occasions. Each node is able to communicate with its neighbor via any one of the available radio interfaces.

Evaluation metrics

Metrics VBPQ, WCETT, AEDT, and ETX(single radio case) are compared using various performance evaluation metrics namely throughput, avg.delay, avg.jitter and Power. A new performance metric called 'Power' of a route has been introduced to evaluate different metrics.

- **Throughput:** This is a very common evaluation metric and often used as a benchmark to compare the performance of new protocols, routing metrics etc. Throughput is defined as the rate of transfer of data successfully from one end to another end. Any route with higher throughput is selected. VBPQ is able to select high throughput routes while WCETT or AETD might take a sub-optimal route even though there is a higher throughput route available.

- **Average delay:** Avg. delay is the average time taken by a packet to reach destination from the source. Any route with lower delay is selected. VBPQ is able to select lower

avg.delay routes while WCETT or AETD might take a sub-optimal route even though there is an optimal route available.

- **Average jitter:** Avg. jitter is the average time difference between consecutive packet transmissions. Any route with lower jitter is selected. VBPQ is able to select lower avg.jitter routes while WCETT or AETD might take a sub-optimal route even though there is an optimal route available. Plots shown in the next few pages reflect the effect of VBPQ on avg.jitter while comparing it with WCETT and AETD under multi-radio scenario and ETX under single radio scenario.

- **Power:** The Power of a route is defined as the ratio of end-end throughput and average delay of that route. Power is expressed in the units of bpss(bits per seconds square). Power of the route is a direct measure to the reliability of that route because of the intuition that higher the power, the better the route and lesser the impact of higher ETTs and hence better the reliability. A route that provides maximum throughput and minimum delay, that is a route with maximum power has to be the first preference for the source node to select a route. VBPQ is able to select routes that have more power while WCETT or AETD might take a sub-optimal route even though there is an optimal route available. Plots shown in the next few pages reflect the effect of VBPQ on power while comparing it with WCETT and AETD under multi-radio scenario and ETX under single radio scenario. Since power is derived from throughput and delay, plots are shown for power instead of both throughput and delay.

To induce an attack, the wireless links are classified into two types: 1) Attacker's links and 2) Normal links. Attacker's links are nothing but the set of links that could together cause the delay-variation attack. In our simulations, the normal links are replaced by the attacker's links and the same set of simulations are carried on the modified network. Results show that the proposed metric VBPQ not only can detect such kind of attacks but also can prevent them where as WCETT and AETD can neither detect nor prevent the attack.

Network parameters: Simulations are carried out by varying the number of hops in both

the single and multi radio cases. In every simulation run, the source sends 10,000 packets each millisecond for 30seconds at constant bit rate. The queue size and the retransmission limits are set to the default values and are set same for all the nodes in the network. The packet size is set to 1024 bytes. To evaluate just the metrics, static routes are employed instead of any routing protocol to avoid any routing overhead to effect the performance evaluation of just the metrics. In multi radio experiments, each node is employed with more than one 802.11 b radios where each propagation channel is set to a different frequency around 2.4 GHz.

In the experiments below, the legends shows the deviation values instead of variance because as the hop number increases variance decreases while the deviation is still constant. To actually compare across various number of hops, deviation is more suitable than variance. To compare metrics for routes of particular length, then variance comes into picture.

4.1.4 Implementation details:

Before going through the simulation results, it is customary to note some of the implementation details and on what preliminary results that the below shown simulation results are based upon and carried out later.

All the scripts are written in Java programming language. These scripts change some of the qualnet scenario files appropriately to carryout the required simulations. All simulations are carried out basing on the following two plots. 1. Distance vs throughput 2. ETT vs throughput

- **Distance vs Throughput:** A script was written in which the distance between two nodes is varied and the throughput at the second node is noted against each value of distance. The graph in Figure 4.3 shows distance vs throughput plots at various datarates.

  It is interesting to see that the throughput is almost constant until some distance and thereon dropping gradually with the increase in distance. This relation is very important for further simulations as it tells how to obtain a certain level of throughput and at what distance.

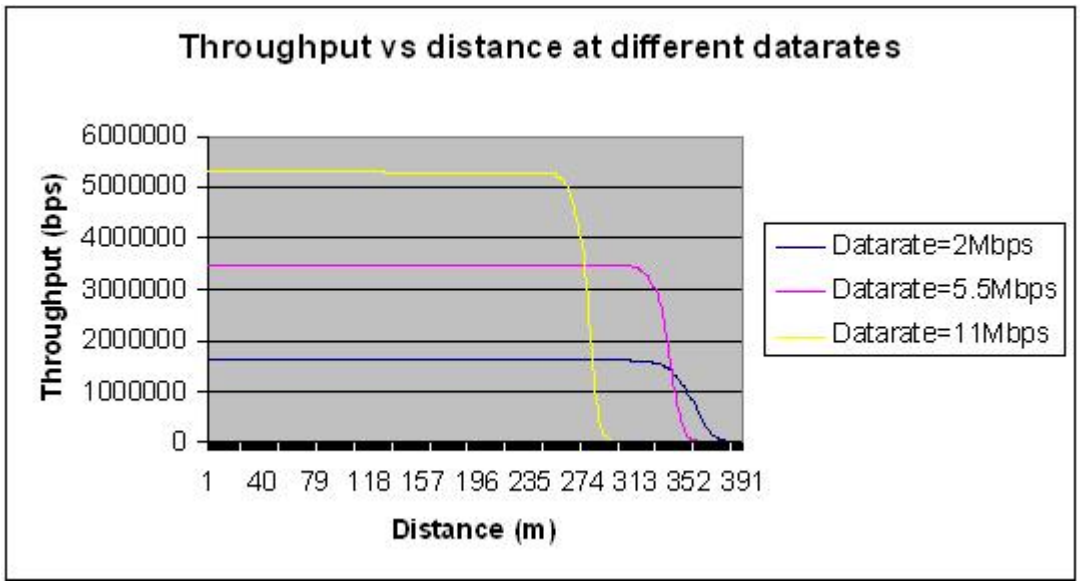


Figure 4.3 **Throughput vs Distance at various data rates. The legend here shows different datarates that qualnet simulator support. Distance is measured interms of meters and throughput in bps.**

- **Distance vs ETT:** ETT is calculated from the simulation itself. For every distance value, all the necessary B and ETX are obtained which inturn are used to calculate ETT.

  S = 1024 bytes

  B = Throughput obtained when two nodes are placed at a distance, can be obtained from the above plots too. This can be considered as the available throughput. In (5), B is calculated using packetpairs technique (31) in which the time taken by two different sized probes is taken into account. Logically if there is some contention on the link or if the nodes move away from each other, then estimated throughput will undoubtedly decrease. Similar logic is followed here but the nodes are moved appropriately to get a different B.

  ETX = (PR+DR+NPR)/NPR where PR and DR correspond to packet and data retransmissions and NPR is the total number of packets received successfully at the server.

  $ETT = S/B * ETX$

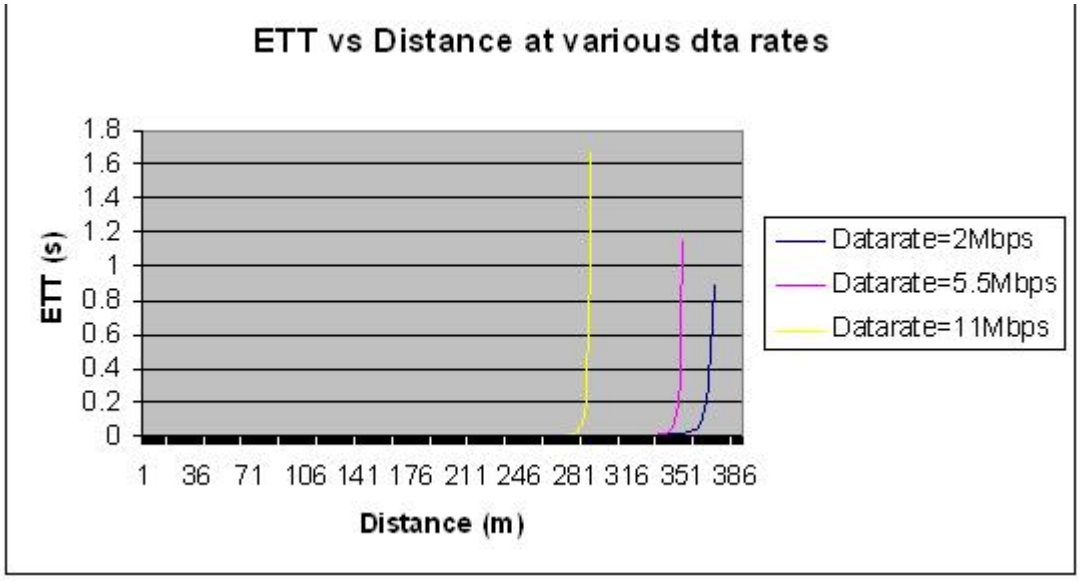


Figure 4.4 **ETT vs Distance at various data rates. The legend here shows different datarates that qualnet simulator support. Distance is measured interms of meters and ETT in s.**

The graph in Figure 4.4 shows Distance vs ETT plots at various datarates.

It is interesting to see that the ETT is almost constant until some distance and there on rising gradually with the increase in distance. This relation is very important for further simulations as it tells how to obtain a certain level of ETT and at what distance. This is how basically normal links are distinguished from the attacker's links.

4.1.5 Simulation Results: Single radio experiments

In this section, results of single radio experiments are presented. VBPQ metric is compared with ETX metric and evaluated in terms of power and avg.jitter. This section also shows that VBPQ outperforms ETX when under delay-variation attack. Each experiment is averaged over 50 simulation runs. Because every node is using only one radio interface, the channel diversity term is zero in the calculations. γ is set to 0.5 to offer a perfect balance between the total expected delay of the route and the expected variation of the route.

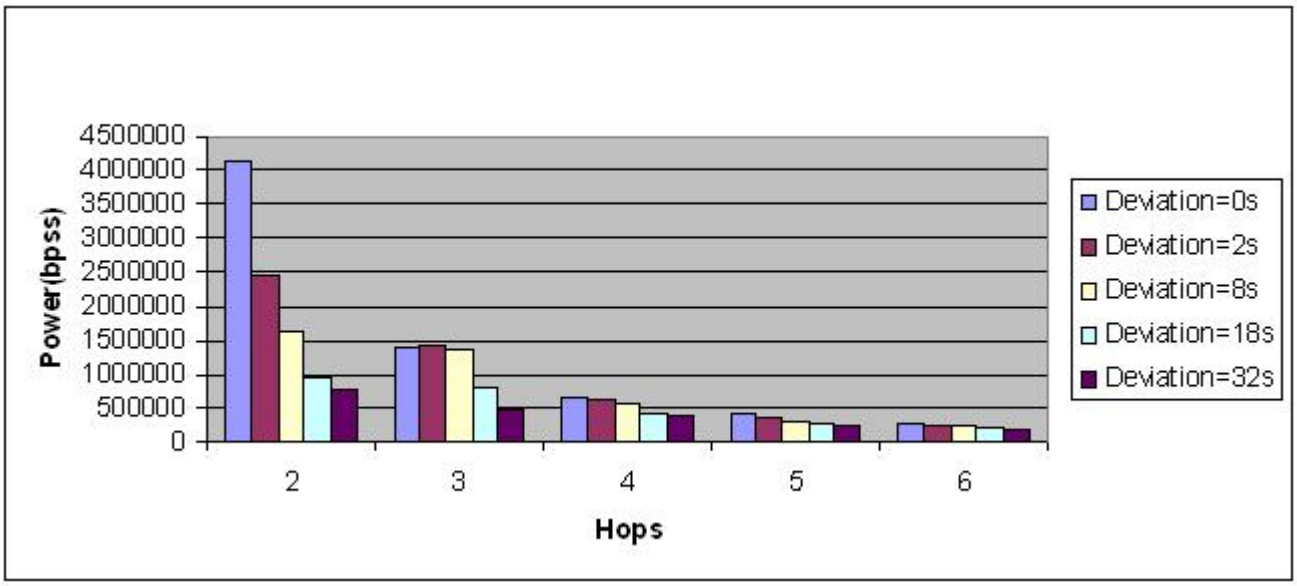


Figure 4.5 **Single Radio: Power comparison at various hop numbers.**

In figure 4.5 the legend shows the deviation values. These deviation values are constant for every hop but the variance varies as hopnumber varies. X-axis shows hop numbers and Y-axis shows power in bpss. The bars on each x-value shows the power if the route has that much deviation(indicated by the corresponding color).

In figure 4.6, the legend shows the deviation values. These deviation values are constant for every hop but the variance varies as hopnumber varies. X-axis shows hop numbers and Y-axis shows avj.jitter in seconds. The bars on each x-value shows the avg.jitter if the route has that much deviation(indicated by the corresponding color).

Figure 4.5 presents the comparison of power for various routes with different lengths and varying variance(deviation) values. For each hop number, the DETT (deviation) of the route ranging from 0 to 32 is varied by keeping the average ETT (=5) and the TETT same. Deviation is used to compare across hops but for a particular hopnumber, variance can be used as the topic of comparison. As can be seen from figure 4.5, as the variance increases , the power of a route decreases. This implies that the lowest variance route will have a better throughput and lower delay when compared to the other routes of same length and same TETT. Since

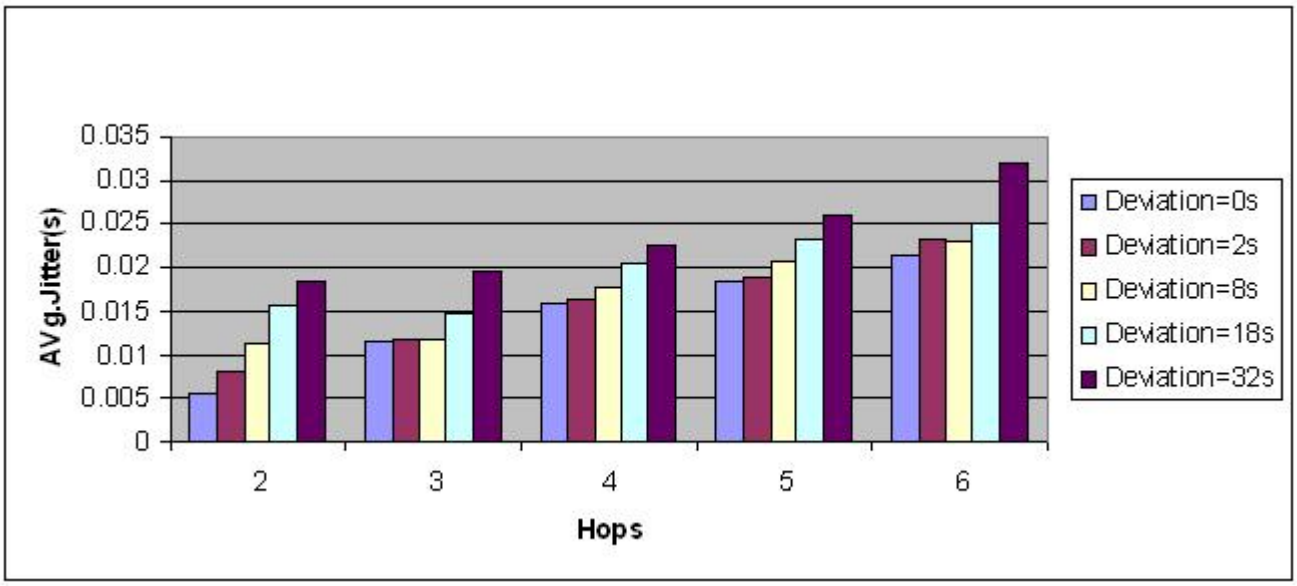


Figure 4.6 **Single Radio: Avg.Jitter Comparison at Various Hop numbers.**

every node is employed with a single radio, the transmission and reception of the packets do not take place simultaneously. So under this scenario, as the hop number increases the power gradually decreases. Figure 4.6 presents the comparison of Avg.Jitter for various routes with different lengths and varying deviation values for every hop. As can be observed from the figure 4.6, as the variance (VETT) increases, the Avg.Jitter increases. This also implies that the lowest variance route will perform better in terms of Avg.Jitter. It can also be seen that the routes with more number of hops will cause the Avg.jitter to increase. This is due to the single radio scenario and also it takes more time between the consecutive transmissions. So for the routes with more number of hops, the lowest variance path performs better than any other path and that means that VBPQ offers better performance better than ETX which might select a suboptimal path.

In figure 4.7, the legend indicates the two metrics VBPQ and ETX under comparison. X-axis represent the hops and Y-axis represent power in bpss. Blue and pink curves represent VBPQ and ETX respectively. Each blue point represents the value of power for a route with a particular length in hops when VBPQ is used and similarly pink point represents ETX.

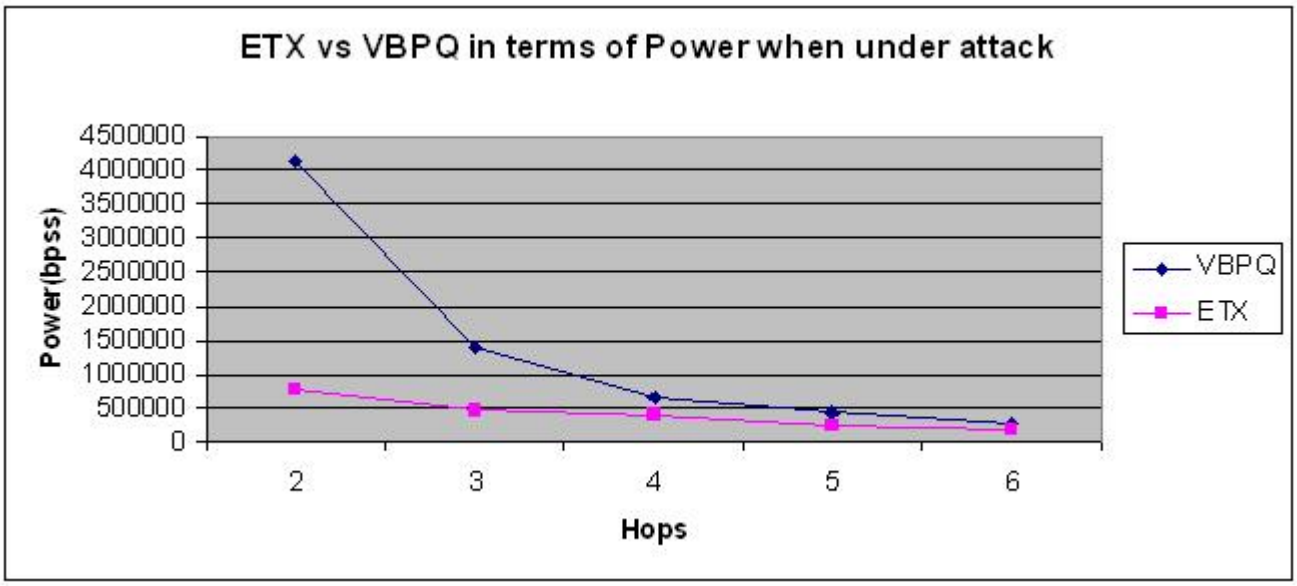


Figure 4.7 **Single Radio: ETX vs VBPQ, Power comparison under attack.**

Figure 4.7 presents the comparison of power metric for ETX and VBPQ when they are in attack. Under the attack, ETX may select a route that has more variance when compared to the one that has lower variance. Figures 4.5 and 4.6 have explained that the variance has a major and prominent role providing a better performance. The lower is the variance, the better is the performance of a network is. VBPQ always tries to select the route with lower variance and henceforth preventing the delay variation attack. Figure 4.7 along with the Figure 4.8 that shows the jitter comparison under attack show that VBPQ out performs ETX at every hop number.

In figure 4.8 the legend indicates the two metrics VBPQ and ETX under comparison. X-axis represent the hops and Y-axis represent avj.jitter in seconds. Blue and pink curves represent VBPQ and ETX respectively. Each blue point represents the value of avg.jitter for a route with a particular length in hops when VBPQ is used and similarly pink point represents ETX.

Figure 4.8 shows the jitter comparison of VBPQ and ETX when the attack is launched.

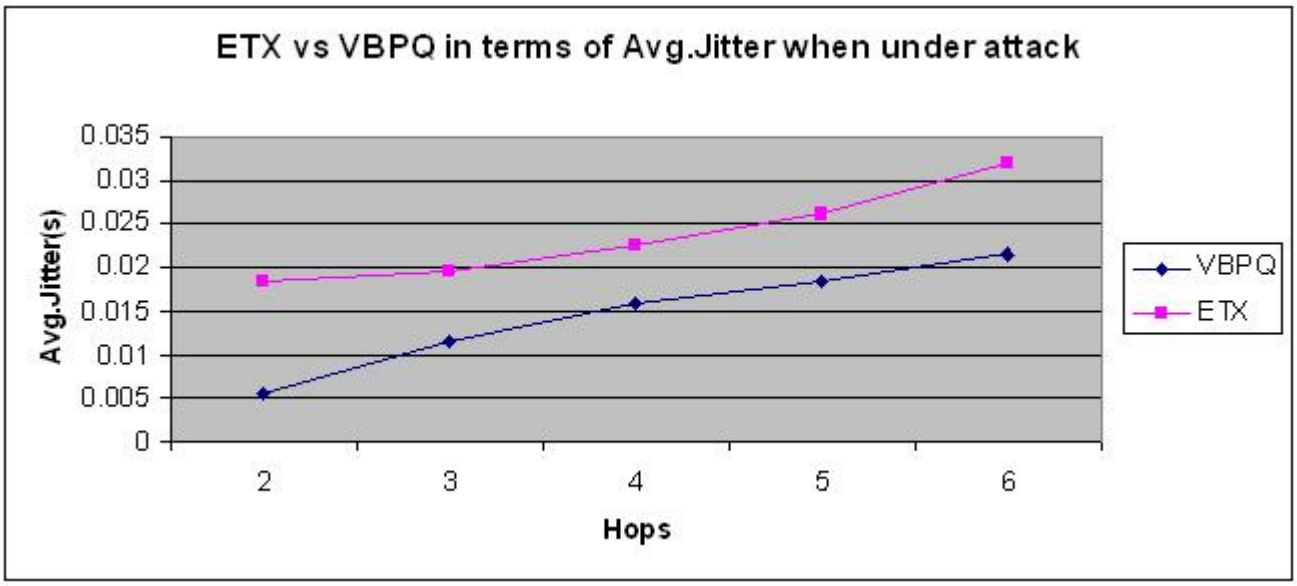


Figure 4.8 **Single Radio: ETX vs VBPQ, Average Jitter comparison under attack**

Even in this experiment, VBPQ gives a lot better performance than ETX under single radio scenario.

4.1.6 Simulation Results: Multi radio experiments-Comparing VBPQ with WCETT and AETD

In this set of experiments, every node is employed with more than one radio. In the previous chapters, the motivation behind coming up with a new metric which might perform better than other metrics like WCETT and AETD is discussed. Now, the rest of this section talks about how much better the proposed VBPQ metric performs when compared to WCETT and AETD metrics. These metrics are evaluated again using power and jitter.

In this section, power and avg.jitter comparison of various metrics namely VBPQ, WCETT and AETD is presented. Before that, the impact of variance on selecting the best route if the underlying metric is WCETT or AETD is presented. WCETT or AETD does not account for the impact that individual link qualities can have on the route selections. The best part of those metrics is the consideration of channel diversity. The total ETT along with is not just

enough to say that these metrics are able to select optimal paths. Variance of a route takes care of the effect of individual link qualities. In this section, it will be shown how variance (VBPQ) is able to select better routes while WCETT or AETD might select some suboptimal routes. Due to space constraints, only the power comparison of the routes with different values of variance is shown. For WCETT, the tuning parameter β is set to 0.5, for AETD α=0.2 and for VBPQ set γ is set to 0.5. In multi radio experiments, each node is employed with 2-4 non interfering (theoretically) 802.11 b radio channels. Here the effect of channel diversity varies according to the metric that calculated it. No special calculation for channel diversity is made, the same formula calculated by the authors of AETD (7) is taken into account.

Figure 4.9 presents the impact of variance on the performance of WCETT. Figure 4.10 presents the impact of variance on the performance of AETD. These figures also show that if variance is considered in the metrics WCETT and AETD, then there will be a huge postive drift in the performance, security and reliability. It is observed at times, AETD and VBPQ perform very similar to each other, in terms of throughput, when the route is composed of more number of hops($\geq$ 5). One of the major factors for this kind of behavior would be the impact of channel diversity of that route compensating the added advantage of the variance of that route. Figure 4.11 shows this kind of behavior. In this case, a random route either selected by our metric or by AETD is chosen.

In figure 4.9 the legend indicates the various deviation values for comparison. X-axis represent the hops and Y-axis represent power in bpss. The bars on each x-value shows the power if the route has that much deviation(indicated by the corresponding color) and if the routing metric is WCETT.

In figure 4.10, the legend indicates the various deviation values for comparison. X-axis represent the hops and Y-axis represent power in bpss. The bars on each x-value shows the power if the route has that much deviation(indicated by the corresponding color) and if the routing metric is AETD.

In figure 4.11 the legend indicates the various deviation values for comparison. X-axis represent the hops and Y-axis represent throughput in bps. The bars on each x-value shows

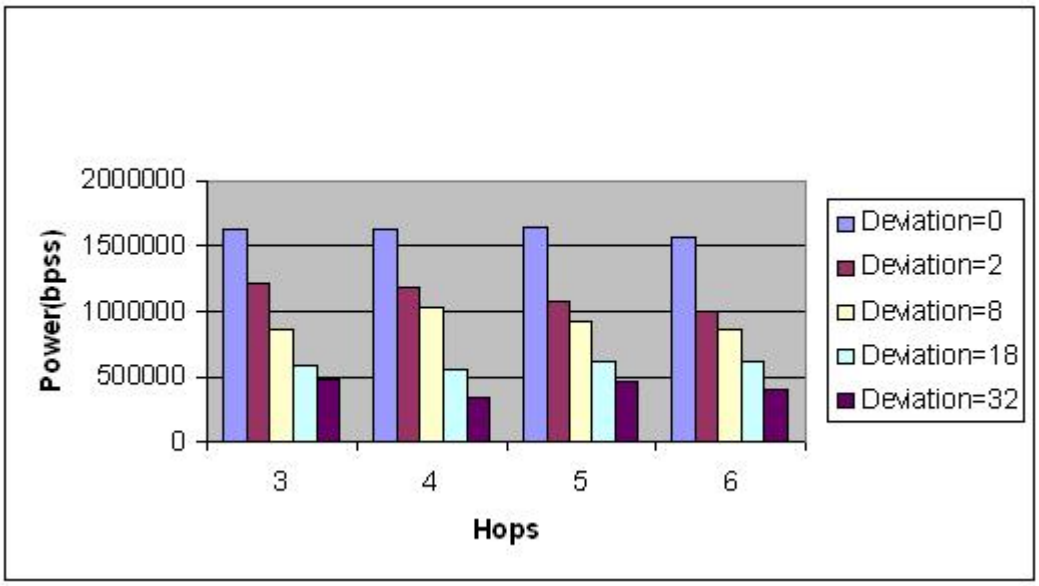


Figure 4.9 **Multi Radio: Effect of variance on the power when the routing metric is WCETT.**

the throughput if the route has that much deviation(indicated by the corresponding color) and if the routing metric is AETD. In this experiment, at hops 5 and 6, VBPQ is not able to select optimal paths and neither is AETD.

Figure 4.12 presents the Power comparison of various metrics when the attack is launched. As one can observe, WCETT is the least performant when compared to AETD and VBPQ. This is because AETD select more channel diverse paths than those selected by WCETT. In addition to this, VBPQ also has this variance factor that helps us to select a better path when compared to AETD. To compare WCETT and AETD, a random route having some WCETT value is selected. Here, we do not change the link qualities, but we change the channel assignment to the links on that route. A more diverse channel assignment would no doubt give a better performace. As one can see in the figure, there is a huge increase in the Power at 4 hops for AETD and VBPQ because consecutive links may be operating on the orthogonal channels. Since a maximum of 4 channels have been employed per node, it may be possible to have a highly channel diverse path that gives a better performance and that has the same value of WCETT as the one selected by WCETT metric. Moreover, in the metric

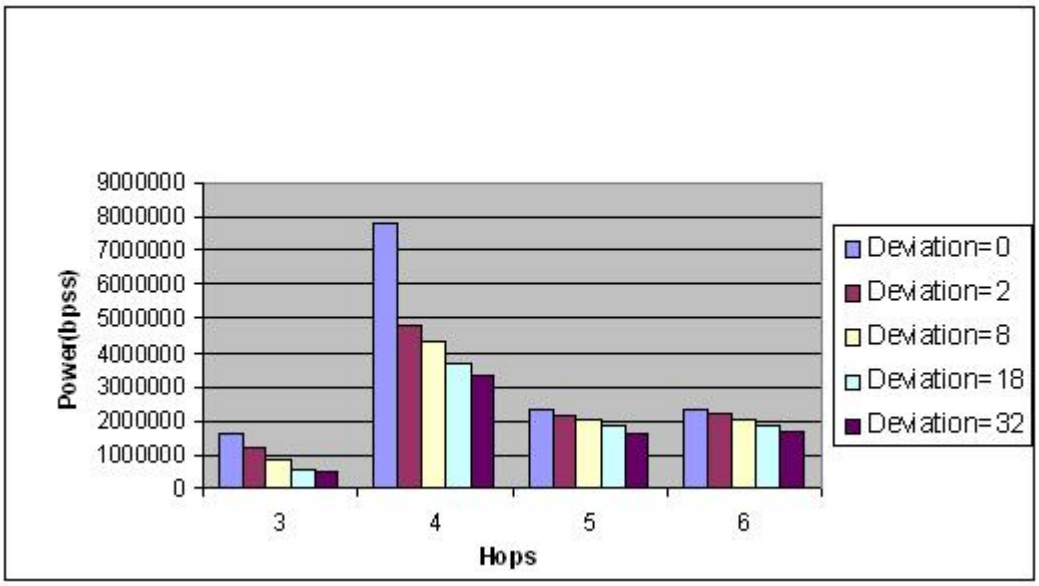


Figure 4.10 **Multi Radio: Effect of variance on the power when the routing metric is AETD.**

VBPQ, AETD is used as the submetric so it supports both channel diverse paths and also low variance paths. It can be observed from Figure 4.12, VBPQ shows a considerable increase in the performance when compared to AETD and WCETT at all the hops.

In figure 4.12 the legend indicates the three metrics VBPQ WCETT, and AETD under comparison. X-axis represent the hops and Y-axis represent power in bpss. Blue,pink and yellow curves represent WCETT, AETD and VBPQ respectively. Each blue point represents the value of power for a route with a particular length in hops when WCETT is used and similarly pink point represents AETD and yellow for VBPQ.

Figure 4.13 presents the Avg.jitter comparison of various metrics when the attack is launched. Even in this figure, VBPQ outperforms both the metrics under comparison. In the above figures 4.12 and 4.13, it is showed that VBPQ performs much better than AETD and WCETT and also is able to prevent the delay-variation attack where as AETD and WCETT are not able to.

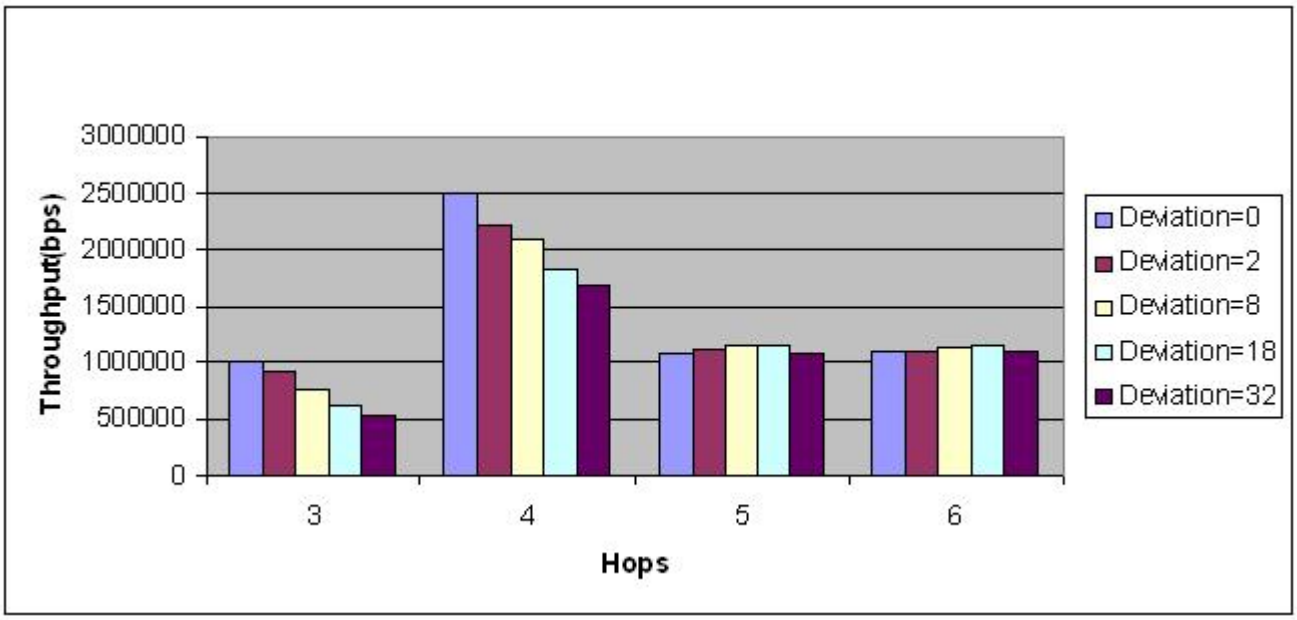


Figure 4.11 **Multi Radio: Effect of variance on the throughput when the routing metric is AETD**

In figure 4.13 the legend indicates the three metrics VBPQ WCETT, and AETD under comparison. X-axis represent the hops and Y-axis represent avg.jitter in seconds. Blue,pink and yellow curves represent WCETT, AETD and VBPQ respectively. Each blue point represents the value of avj.jitter for a route with a particular length in hops when WCETT is used and similarly pink point represents AETD and yellow for VBPQ.

The results confirm that the proposed metric VBPQ outperforms various metrics both in single radio and also multi radio scenarios. The results also confirm to the mathematical analysis of the metric. VBPQ not only is able to prevent the delay variation attack introduced in the paper but also is able to provide much better throughput, power, delay and jitter. This shows that the routing protocol that uses the metric VBPQ is not only secure but also reliable and robust in nature.

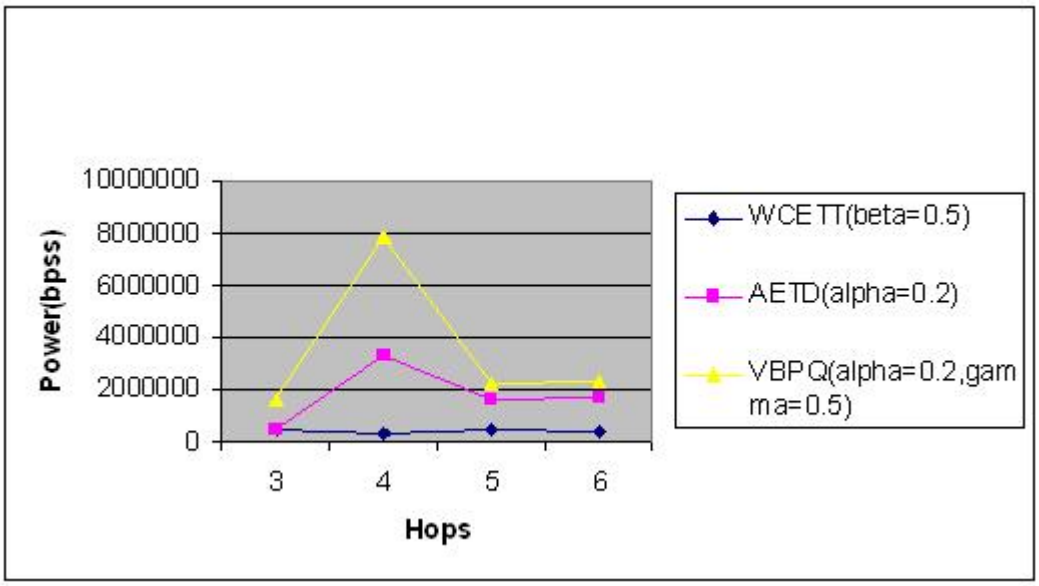


Figure 4.12 **Multi Radio: Power Comparison of VBPQ, AETD and WCETT under delay-variation attack**

4.2 Results: WHDetect

In this section, various plots reflect the detection of wormhole attack anamolies using two different methods namely average probability method and average count method. As mentioned in the previous sections, WHDetect uses a data mining approach called cross feature analysis. This approach is done in several stages. Each stage is discussed in the light of obtaining the data for the results.

- **Training data set:** Training data set that contain normal entries is obtained from the simulator Qualnet. A simulation set up that was followed in the previous section is used. The network parameters are also same except for the fact that the simulation time and sampling period are not constant. They are used as features in the feature set so they tend to have different values at different points of the experiment. The size of the training data set depends on how the features are extracted?, what features are being selected?, are the features continuous or discrete?. Next immediate step is the feature set construction.

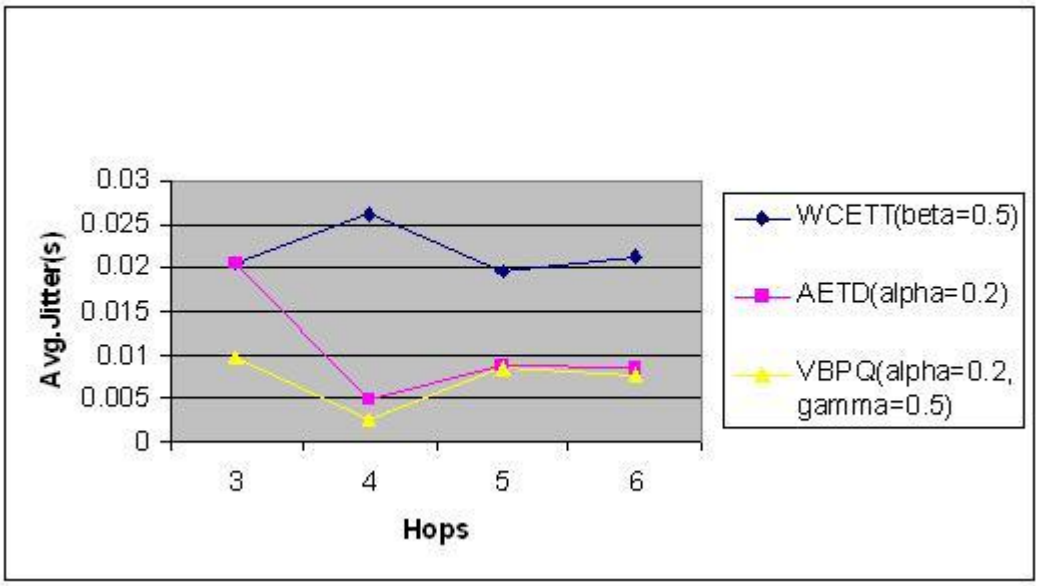


Figure 4.13 **Multi Radio: Avg.Jitter Comparison of VBPQ, AETD and WCETT under delay-variation attack**

- **Feature set construction:** For the detection of wormhole attack in link quality based source routing protocols, the two important features are distance and ETT. Is there any relation between them or can we obtain any? is the point of question. Yes, as the distance increases after a certain point, ETT also increases. It is a simple intuition that as the distance between two nodes connected by a wireless link increases, more noise adds up to the transmissions reducing the link quality and there by increasing ETT. But the problem with distance and ETT are that they are continuous. Distance can take any value between 0 and 504 m (max transmission range possible from the simulation setup used.). ETT can take any positive real number. These two features are discretized into five intervals each. The division of ETTs and distances into intervals is made fair and suitable. Each interval is termed as a bucket. Values falling under a certain interval will be assigned the bucket index corresponding to the interval. Table 4.1 shows how the continuous domains of distance and ETT are discritized into buckets.

  The other features are packet size, datarate, sampling period, simulation time. The experiments are carried by varying the number of features. In the first set of experiments,

Distance until (m)	Distance Bucket index	ETT until (ms)	ETT Bucket index
245	0	5	0
279	1	15	1
300	2	20	2
350	3	30	3
>350	4	>30	4

Table 4.1 **Discretization of distance and ETT domains**

first four features are used and in the next, first five are used and in the last experiment all the six features and the impact of their correlation on recall and precision have been noted. The list of features is as shown in 4.2. Table 4.2 also shows the bucket index corresponding to the possible values of the features.

Features	Values
Distance	0,1,2,3,4
ETT	0,1,2,3,4
Packetsize in bytes (index)	512(0), 1024(1)
Datarate in Mbps (index)	1(0), 2(1), 5.5(2), 11(3)
Sampling rate in ms (index)	1(0), 100(1), 200(2)
End time in s (index)	30(0), 90(1), 150(2)

Table 4.2 **Feature set construction**

- **Building submodels**: The next step is to build submodels. Each submodel targets one feature and predicts its class for all combinations of other features. In table 4.3, a submodel that predicts the class of ETT for all possible combinations (only some are shown) of other features is shown. Like this there would be as many submodels as the number of features.

Distance	Packet Size	Data rate	ETT (predicted)
0	0	0	0
1	1	3	2
1	0	3	1
3	1	2	3

Table 4.3 **A submodel targeting ETT**

- Training process and threshold determination: After the submodels are built, the normal

data is fed into the above set of submodels to determine if the normal data is able encapsulate all the submodels with good probability or count. There are two methods of classification employed here.

- Average count method: Any entry is fed into the submodel detection system, where a counter is maintained and incremented as the entry finds itself in each submodel. The counter is normalized by dividing itself with the number of features.
- Average probability method: Any entry is fed into the submodel detection system, where a probability value is assigned depending on in how many submodels this entry is present and how often the predicted value is matched with the actual value.

After the normal data is classified and assigned the corresponding counts and probabilities, a threshold is determined. A minimum count or probability of all entries is selected as the threshold depending on the classification method used. Actually, in the plots sections one can see the data points are various threshold values. But as the threshold value is increased, it is observed that the false alarm rate is rising.

- **Generating random data and detecting anamolies**: This is the final step of cross feature analysis for detecting worm hole attacks in link quality based source routing protocols. Firstly random data is generated that contains both normal and abnormal data. Each data object is classified as normal or abnormal based on the threshold determined in the previous step. If not they are categorized as false alarms.

4.2.1 Implementation details and plots

In this section, implementation details and plots are discussed.

4.2.1.1 Implementation:

The cross feature analysis for detecting wormhole attack is implemented in Java. See Figure 4.14 for the graphical user interface developed for the user to go through each stage of the cross feature analysis. In this figure, first get the training data or simulated data and

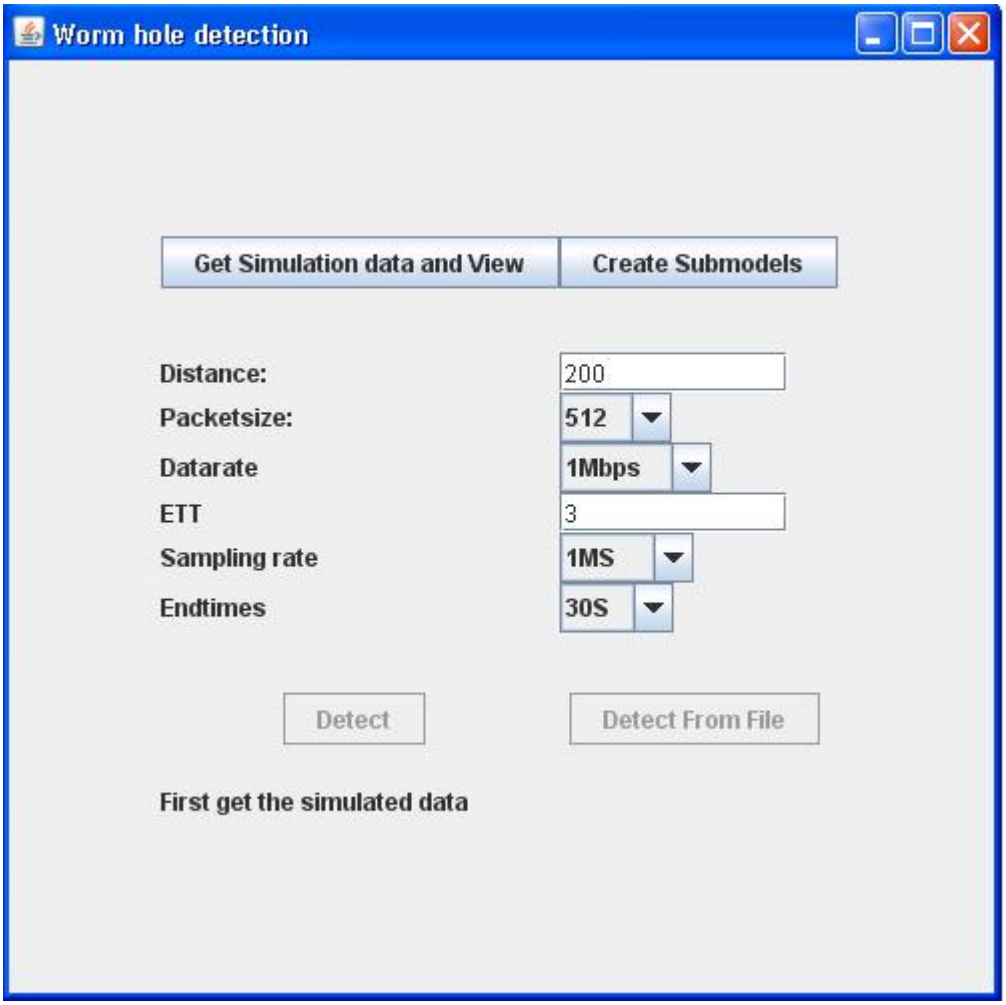


Figure 4.14 **Wormhole attack detection: GUI**

then create submodels. After that, enter the values of each feature and build a feature vector. Press Detect to see if that is normal or abnormal. User will be notified if it is an anamoly or normal (not shown in the figure). There is one more way, that is "'Reading from file"' where a file containing random data is fed into the submodels instead of one at a time. A table (not shown here) will be shown that shows whether or not each data entry is abnormal.

4.2.1.2 Plots:

In this section, plots are drawn for probability and count methods. In each plot, at various threshold values, and using different feature sets, recall and precision values are plotted. The

results show that the plots for probability method are very convincing in finding the anamolies correctly. Table 4.4 shows how normal, abnormal and false alarms are determined. A positive object is a properly detected anamoly and a negative object is a properly detected normal event. When in the test, an object's predicted class is not matching with the actual class, false alarms like false positives and false negatives are generated. This type of classification is helpful in formulating recall and precision.

Test/Actual	True	False
True	True Positive (TP)	False Positive (FP)
False	False Negative (FN)	True Negative (TN)

Table 4.4 **Determining anamolies**

Definitions:

- **Recall:** Recall is a measure of fraction of known positive objects that are correctly classified. That means if attack detection is considered positive, then recall calculates the fraction of the number of known attacks that are correctly classified as anamolies in the testing environment using cross feature analysis.

  Recall = TP/(TP + FN)

- **Precision:** Precision is a measure of fraction of classified positive objects that are truly positive. That means if attack detection is considered positive, then precision calculates the fraction of the number of detected anamolies(from the testing environment) that are actually anamolies.

  Precision = TP/(TP + FP)

Plots: There are two plots shown here. See figures 4.15 and 4.16.

- In figure 4.15, the X-axis shows the recall values and Y-axis shows precision values. The legend shows three experiments involving different feature sets. The points on the curves indicated in (yellow, blue and pink) are different thresholds ranging from 0.5 to 0.95. For some threshold values, the curve data is same so those points are not repeated. The recall

values are not so good when the threshold values are low. Generally a threshold of 0.20 is considered to be decent. The recall values at this point are very low for count method but the precision values are good. That means, there are many false negatives but no false positive at this point. As the threshold value is increased further, the precision is decreasing and recall is increasing. At higher thresholds, recall goes to 1 but undesired as the false positives increase.

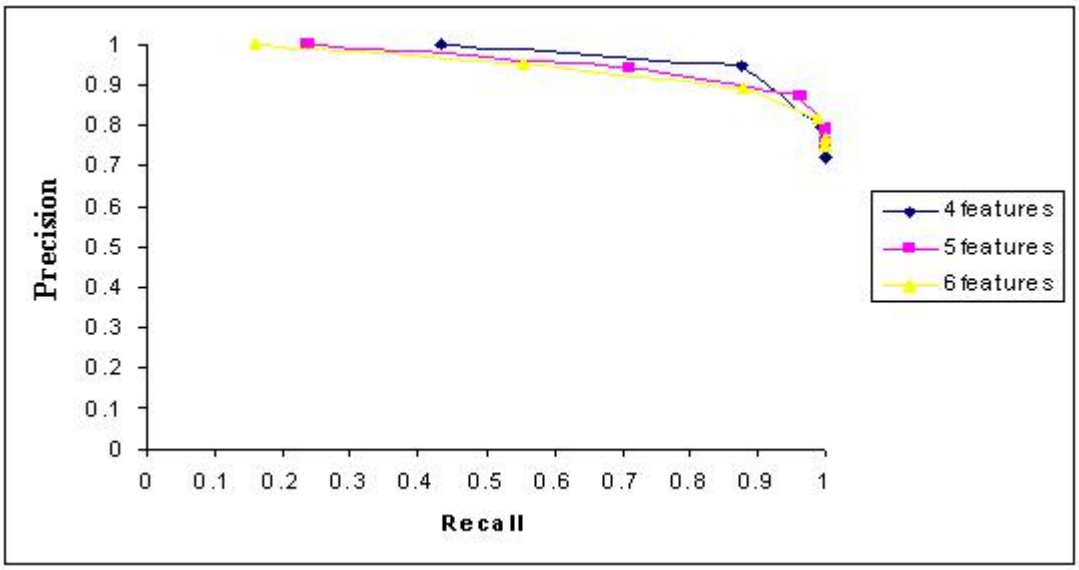


Figure 4.15 **Recall vs Precision curves, when count method was used at various thresholds and for different feature sets**

- In figure 4.16, the X-axis shows the recall values and Y-axis shows precision values. The legend shows three experiments involving different feature sets. The points on the curves indicated in (yellow, blue and pink) are different thresholds ranging from 0.5 to 0.95. For some threshold values, the curve data is same so those points are not repeated. The recall values is always 1 at all threshold values. Generally a threshold of 0.20 is considered to be decent. Even the precision values are really good ranging from 0.9 to 0.7. That means, there are no false negatives but a few false positives at all threshold points. As the threshold value is increased further, the precision is decreasing and recall stays at 1.

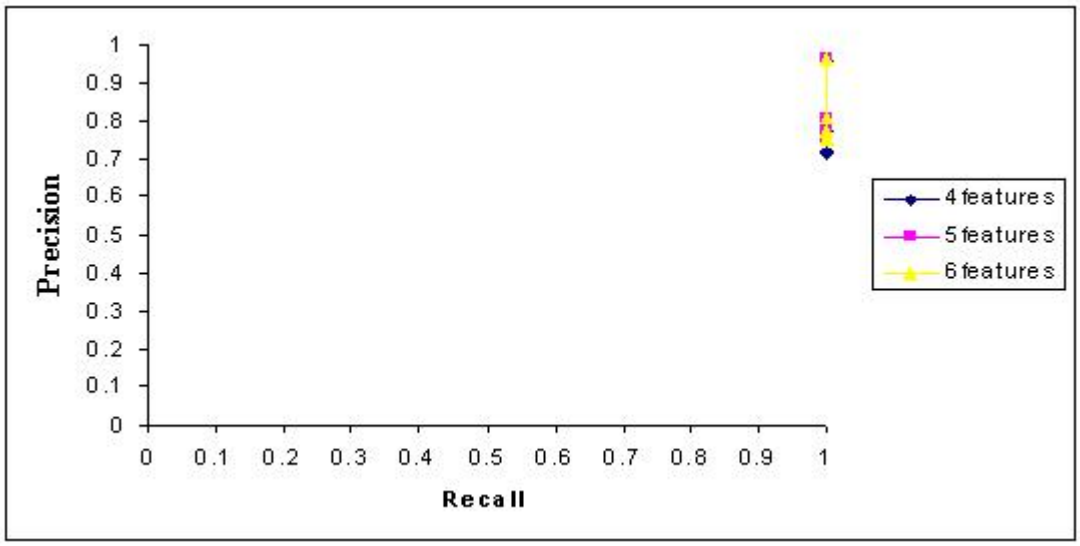


Figure 4.16 **Recall vs Precision curves, when prob method was used at various thresholds and for different feature sets**

- **Observations:** Probability method outperforms count method. Recall rate for probability method is 1 which indicates that known anamolies are always correctly classified independent of the threshold value, but there are some false positives increasing as the threshold value increases. This shows us that a threshold value as low as .1 to 0.2 is good enough. Count method if employed is generating more false alarms than probability method.

CHAPTER 5 CONCLUSIONS

5.1 Summary

The main goal of this thesis is to study the security and routing aspects of wireless ad hoc and mesh networks. Wireless ad hoc networks are highly vulnerable to attacks as they have no centralized system to manage subtle and highly important requirements like security, scalability, network throughput, etc. This thesis mainly concentrates on security, reliability and network throughput. This thesis has two main contributions. First contribution is a new routing metric called Variance based path quality metric (VBPQ) for link based routing protocols. Second contribution is an algorithm that detects worm hole attacks while the underlying routing protocol is any link quality based source routing protocol.

5.1.1 Variance Based Path Quality metric (VBPQ)

Previous link quality metrics for multi-radio multi-hop wireless ad hoc and mesh networks like WCETT, AETD etc do not consider the effect of individual link qualities on the total route quality and route selection. This lack of ability from WCETT or AETD would allow them to select suboptimal paths when actually an optimal path is available. This work also introduces a possible attack called delay-variation attack which can be classified as a routing disruption attack. To be specific, it can be launched by a couple of colluding attackers attracting packets at one point by showing very good link qualities and dropping packets at the other end by decreasing the link quality. This can also be classified as a colluding blackhole attack. VBPQ metric is especially designed for this kind of scenario where it provides a robust, reliable and secure edge to the routing mechanism. Variance ETT is kind of both a secure metric and a reliable metric in this sense. Security is provided without incurring any overhead and without

hindering any performance of the network. Results show that VBPQ outperforms WCETT and AETD in multi-radio scenario and ETX in single-radio scenario in terms of power, throughput, delay and jitter. Power is the ratio of throughput and delay. So higher the power, better the route.

5.1.2 WHDetect: Algorithm that detects Wormhole attack

WHDetect is designed and implemented to detect wormhole attack in link quality based source routing protocols. The algorithm employs a data mining approach called cross feature analysis proposed in (23). The authors in (23) have evaluated their metric on DSR and AODV in detecting black hole attacks and other packet dropping attacks. Algorithm WHDetect uses the same approach but with different feature sets that are more suitable to detecting wormhole attacks. An ETT profile is maintained at every node and this algorithm is executed whenever a node receives a route reply packet to check if this packet was originated from a legitimate node. In the results section, recall and precision curves are shown for various thresholds and for various feature sets. Recall values when probability method is employed are always 1 which says that there are false negatives. So this allowed the algorithm to select probability method to classify the data as normal or abnormal. WHDetect is able to detect all the anamolies except that there are a very few false positives.

5.2 Future Work:

As part of future work, the whole range of attacks that are possible in wireless mesh networks can be studied, and how the metric (VBPQ) can give a solution to them can be examined. Secondly, privacy issues in multihop networks using the metric (VBPQ) can be addressed. Since variances of the paths are used, the data can be distributed along disjoint paths (with same TETTs) in the ratio of their variances so that it is hard for an attacker to assemble data and get the whole information at any point of time. For the detection of wormhole attack, a data mining approach called 'cross feature analysis' has been employed and an algorithm has been designed that takes only a set of 4-6 features into account. This

algorithm may be evaluated with respect to other features related to MAC layer, transport layer, etc. Since the algorithm WHDetect has been devised for link quality based routing protocols, research may be conducted to test if it can be generalized to all source routing protocols.

BIBLIOGRAPHY

[1] Ian F. Akyildiza, Xudong Wangb, and Weilin Wangb (2005). Wireless mesh networks: a survey. *IEEE Radio Communications*

[2] Xudong Wanga, and Azman O. Limb. (2007) IEEE 802.11s wireless mesh networks: Framework and challenges. *Journal of Ad hoc networks*

[3] Xudong Wanga, Edward Knightlyb, Marco Contic, and Anthony Ephremidesd.(2007) A Special issue on wireless mesh networks *Journal of Ad hoc networks*

[4] D. D. Couto, D. Aguayo, J. Bicket, and R. Morris. A high-throughput path metric for multi-hop wireless routing. *ACM MobiCom 2003.*

[5] Richard Draves, Jitendra Padhye, and Brian Zill. Routing in multi-radio, multi-hop wireless mesh networks. *International Conference on Mobile Computing and Networking. Proceedings of the 10th annual international conference on Mobile computing and networking*

[6] V. Bahl, R. Chandra and J. Dunagan. SSCH: Slotted seeded channel hopping for capacity improvement in IEEE 802.11 ad-hoc wireless networks *ACM MobiCom 2004.*

[7] Wei Zhou, Dongbo Zhang, and Daji Qiao. Comparative study of routing metrics for multi-radio multi-channel wireless networks. *WCNC 2006.*

[8] David B. Johnson, David A. Maltz and Josh Broch. DSR: The dynamic source routing protocol for multi-hop wireless ad hoc networks. *In Ad Hoc Networking, edited by Charles E. Perkins, chapter 5, pages 139–172. Addison-Wesley, 2001. http://citeseer.ist.psu.edu/johnson01dsr.html*

[9] Jangeun Jun and Mihail L. Sichiti. The nominal capacity of wireless mesh networks. *Wireless Communications, IEEE [see also IEEE Personal Communications], 2003 Volume: 10, Issue: 5, On page(s): 8- 14*

[BelAir] BelAir Networks white paper. Capacity of wireless mesh networks. Understanding single radio, dual radio and multi-radio wireless mesh networks. *http://www.belairnetworks.com/resources/pdfs/Mesh_Capacity_BDMC00040-C02.pdf*

[Qualnet] QualNet Simulator, http://www.scalable-networks.com/, Online Link.

[802.11b] IEEE 802.11b, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: high-speed physical layer extension in the 2.4 GHz band. *Supplement to IEEE 802.11 Standard, Sept. 1999.*

[10] Azzedine Boukerche. Performance Evaluation of Routing Protocols for Ad Hoc Wireless Networks . *Mobile Networks and Applications Volume 9 , Issue 4, Pages: 333 - 342*

[11] C.E.Perkins and P. Bhagwat. Highly Dynamic Destination-Sequenced Distance Vector (DSDV). *Mobile Computers Proc. of the SIGCOMM 1994 Conference on Communications Architectures, Protocols and Applications, Aug 1994, pp 234-244.*

[12] Phillippe Jacquet, Paul Muhlethaler, Amir qayyum, Anis Laouiti, Laurent Viennot and Thomas Clausen. Optimized Link State Routing Protocol (OLSR) http://www.olsr.net/, http://www.olsr.org/ *RFC 3626,2003*

[13] Shree murthy and J.J.Garcia-Luna-Aveces. WRP (Wireless Routing Protocol)-A Routing Protocol for Packet Radio Networks. *Proc. ACM International Conference on Mobile Computing and Networking, pp. 86-95, November, 1995 AACM/Baltzer Journal on Mobile Networks and Applications, Special Issue on Routing in Mobile Communication Networks, Vol. 1, No. 2, pp 183-197, ACM, October 1996*

[14] C.E. Perkins and E.M. Royer. Ad-hoc on-demand distance vector routing (AODV) *Proc. of 2nd IEEE Workshop on Mobile Computing Systems and Applications (1999).*

[15] Sanzgiri, K. Dahill, B. Levine, B.N. Shields and C. Belding-Royer. A secure routing protocol for ad hoc networks. (ARAN) *Network Protocols, 2002. Proceedings. 10th IEEE International Conference on ICNP'02*

[16] Manel Guerrero Zapata. Secure ad hoc on-demand distance vector routing.(SecAODV) *ACM SIGMOBILE Mobile Computing and Communications Review (2002)*

[17] Yih-Chun Hu, Adrian Perrig, and David B. Johnson. Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks. *Proceedings of the Eighth Annual International Conference on Mobile Computing and Networking (MobiCom 2002), pp. 12-23, ACM, Atlanta, GA, September 2002.*

[18] Yih-Chun Hu, Adrian Perrig, and David B. Johnson. Rushing attacks and defense in wireless ad hoc network routing protocols. *Workshop on Wireless Security. Proceedings of the 2nd ACM workshop on Wireless security. 2003*

[19] C.Y Hu, A. Perrig and D.B Johnson. Packet leashes: a defense against wormhole attacks in wireless networks. *INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies. IEEE*

[20] I. Khalil and N.B Saurabh Bagchi Shroff. LITEWORP: A lightweight countermeasure for the wormhole attack in multihop wireless networks. *Dependable Systems and Networks, 2005. DSN 2005.*

[21] Lijun Qian, Ning Song and Xiangfang Li. Detecting and locating wormhole attacks in wireless ad hoc networks through statistical analysis of multi-path. *Wireless Communications and Networking Conference, 2005 IEEE*

[22] Xia Wang and J. Wong. An end-to-end detection of wormhole attack in wireless ad-hoc networks. *Proceedings of the 31st Annual International Computer Software and Applications Conference - Vol. 1- (COMPSAC 2007)*

[23] Yi-an Huang, Wei Fan, Wenke Lee, and Philip S. Yu. Cross-Feature analysis for detecting ad-hoc routing anomalies. *In Proceedings of The 23rd International Conference on Distributed Computing Systems (ICDCS), Providence, RI, May 2003.*

[24] White Paper [2005] : An Introduction to Wireless Mesh Networking *Firetide, Inc. www.firetide.com*

[25] Jakob Eriksson, Sharad Agarwal, Paramvir Bahl and Jitendra Padhye. Feasibility study of mesh networks for all-wireless offices. *http://research.microsoft.com/ sagarwal/mobisys06.pdf International Conference On Mobile Systems, Applications And Services. Proceedings of the 4th international conference on Mobile systems, applications and services*

[26] Raffaele Bruno, Marco Conti, and Enrico Gregori. National Research Council (CNR): Mesh Networks: Commodity multihop ad hoc networks. *http://ieeexplore.ieee.org/iel5/35/30467/01404606.pdf Communications Magazine, IEEE Volume: 43, Issue: 3 On page(s): 123- 131*

[27] Y. Yang, J. Wang, and R. Kravets. Designing routing metrics for mesh networks. *IEEE Workshop on Wireless Mesh Networks (WiMesh),Sept. 2005.*

[28] C. E. Koksal and H. Balakrishnan. Quality-aware routing metrics for time-varying wireless mesh networks. *IEEE Journal on Selected Areas in Communications, vol. 24, no. 11, pp. 19841994, Nov. 2006.*

[29] L. R. Ford Jr. and D. R. Fulkerson. Flows in networks *Princeton Univ.Press, 1962.*

[30] A.P Subramanian , M.M Buddhikot and S. Miller. Interference aware routing in multiradio wireless mesh networks *Wireless Mesh Networks, 2006. WiMesh 2006. 2nd IEEE Workshop on Volume , Issue , 2006 Page(s):55 - 63*

[31] S. Keshav. A Control-theoretic approach to flow control. *SIGCOMM, 1991.*

[Data mine] Data mine by Andy Pryle. http://www.the-data-mine.com/

[32] J.A. Hartigan and M.A. Wong. Algorithm AS 136: A K-Means clustering algorithm *Applied Statistics, Vol. 28, No. 1 (1979), pp. 100-108*

[33] Terran Lane and Carla E. Brodley. Temporal sequence learning and data reduction for anomaly detection. *ACM Transactions on Information and System Security*