

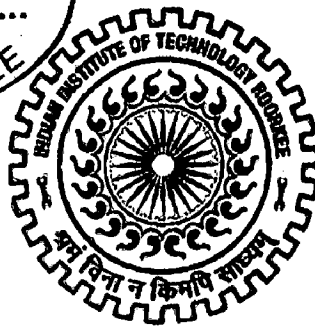
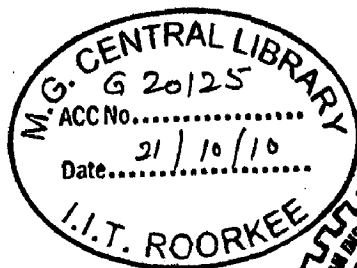
**IMPLEMENTATION OF A SECURE TRUST MODEL
FOR
POWER AWARE AODV ROUTING IN MANETS**

A DISSERTATION

*Submitted in partial fulfillment of the
requirements for the award of the degree
of
MASTER OF TECHNOLOGY
in
COMPUTER SCIENCE AND ENGINEERING*

By

NAGA SATHISH GIDIJALA



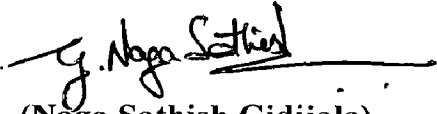
**DEPARTMENT OF ELECTRONICS AND COMPUTER ENGINEERING
INDIAN INSTITUTE OF TECHNOLOGY ROORKEE
ROORKEE -247 667 (INDIA)
JUNE, 2010**

Candidate's Declaration

I hereby declare that the work being presented in the dissertation report titled "Implementation of a Secure Trust Model for Power Aware AODV Routing in MANETs" in partial fulfillment of the requirement for the award of the degree of Master of Technology in Computer Science and Engineering, submitted in the Department of Electronics and Computer Engineering, Indian Institute of Technology Roorkee, is an authentic record of my own work carried out under the guidance of Dr. Ramesh C Joshi, Professor in the Department of Electronics and Computer Engineering, Indian Institute of Technology Roorkee. I have not submitted the matter embodied in this dissertation report for the award of any other degree.

Dated: 09-06-2010

Place: IIT Roorkee

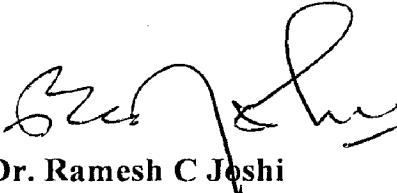

(Naga Sathish Gidijala)

Certificate

This is to certify that above statements made by the candidate are correct to the best of my knowledge and belief.

Dated: 09-06-2010

Place: IIT Roorkee.


Dr. Ramesh C Joshi

Professor,

Department of Electronics and Computer
Engineering,

IIT Roorkee, Roorkee,

247667 (India)

ACKNOWLEDGEMENTS

I am thankful to Indian Institute of Technology Roorkee for giving me this opportunity. It is my privilege to express thanks and my profound gratitude to my supervisor Dr. Ramesh C Joshi, Professor for his invaluable guidance and constant motivation throughout the dissertation. I was able to complete this dissertation in time due to the constant motivation and support received from him.

I would like to thank Dr. Manoj Mishra and Dr. A. Patnaik for their valuable suggestions and guidance for the successful completion my dissertation work. I would also like to thank Dr. Kum Kum Garg for allowing me to attend the National Conference for oral presentation of the selected paper. I am grateful to Mr. Tirumalesh, Mr. Appala Raju and Mr. Sai Deepak, my seniors, for their valuable help and constant support. I am also thankful to all my friends who helped me directly and indirectly in completing this dissertation.

Most importantly, I would like to extend my deepest appreciation to my family for their love, encouragement and moral support.



(Naga Sathish Gidijala)

ABSTRACT

MANET refers to a network formed by a group of wireless mobile nodes that can communicate with each other and also mobile at the same time. MANET is an infrastructure-less network in which all the mobile nodes cooperate with each other in routing packets from source node to the destination nodes, in accordance with some routing protocol.

The main goal of this dissertation work is to provide secure energy efficient routing protocol based on trust modeling for mobile ad hoc networks, since the critical limiting factors for a mobile node is its operation time, restricted by battery capacity and trusted third party, the absence of which may result in nodes deviating from the routing protocol for selfish or malicious reasons.

This work addresses both these problems in MANETs by proposing a new robust trust mechanism against route misbehavior attacks over energy efficient AODV routing. The performance of the proposed methodology has been studied on simulated environment using JiST-SWANS with ad hoc network comprising of route misbehavior attacks.

TABLE OF CONTENTS

Candidate's declaration.....	i
Certificate.....	i
Acknowledgements.....	ii
Abstract.....	iii
Table of Contents.....	iv
List of Figures	vi
List of Tables.....	vii

CHAPTER 1: INTRODUCTION AND PROBLEM STATEMENT..... 1

1.1 Motivation.....	3
1.2 Problem Statement.....	4
1.3 Organization of report.....	5

CHAPTER 2: BACKGROUND AND LITERATURE REVIEW..... 7

2.1 Ad Hoc On-demand Distance Vector Routing and its Energy Issues.....	7
2.1.1 Overview of the Ad Hoc On-demand Distance Vector (AODV) Protocol..	7
2.1.2 Metrics for Energy Aware Routing.....	10
2.1.3 Energy-Aware Routing Based on AODV.....	11
2.1.4 Power Conserving Methods at Various Layers of Protocol Stack.....	13
2.2 Background for Trust Based Systems.....	14
2.2.1 The Notion of Trust.....	14
2.2.2 Difference between a Trust System and a Reputation System.....	16
2.2.3 Survey of Various Existing Trust Models.....	18

CHAPTER 3: DESIGN DETAILS OF PROPOSED TRUST MODEL.....	20
3.1 Overall Design Strategy.....	20
3.2 Design of Attack Modules.....	23
3.3 Design of Energy Model.....	26
3.4 Proposed Framework for Robust Trust Mechanism.....	28
CHAPTER 4: SIMULATION AND IMPLEMENTATION DETAILS.....	35
4.1 Java in Simulation Time (JiST) Engine Architecture.....	35
4.2 Scalable Wireless Ad hoc Network Simulator (SWANS).....	36
4.3 Simulation Set Up and Implementation.....	39
CHAPTER 5: RESULTS AND ANALYSIS.....	42
CHAPTER 6. CONCLUSION AND FUTURE WORK.....	46
6.1 Conclusion.....	46
6.2 Future Directions.....	47
REFERENCES.....	49
LIST OF PUBLICATIONS.....	53

List of Figures

Fig.2.1	Generalized MANET Topology	11
Fig 2.2	Trust transitivity principle.....	17
Fig 3.1	Overall Design Strategy for Robust Secure Trust Model	22
Fig 3.2	Working of Blackhole On Route Attack.....	24
Fig 3.3	Working of Blackhole Fake Dest Reply Attack.....	25
Fig 3.4	Working of GreyHole Attack.....	26
Fig 3.5	Selection of Shortest, Most Trustable and Energy Efficient Route out of available routes	29
Fig 3.6	Working of packetBuff DataStore while Forwarding a Packet to the Neighbour.....	30
Fig 3.7	Routing Decision Methodology at Intermediate Nodes (Routers).....	32
Fig 3.8	Route Selection Methodology among various available routes at the Destination Node.....	33
Fig 4.1	Alternative spatial data structures for radio signal propagation.....	38
Fig 5.1	Throughput comparison with varying number of malicious nodes following specified attacks on AODV.....	42
Fig5.2	Throughput comparison with varying number of malicious nodes following specified attacks on Simple Trust Model without considering Battery Energy for Routing Decisions.....	43
Fig 5.3	Throughput comparison with varying number of malicious nodes following specified attacks on Secure Trusted Power Aware AODV.....	44

List of Tables

Table 2.1	Methods to Conserve Power at Various Protocol Layers.....	13
Table 4.1	Parameters Values used in Simulation.....	40

Chapter 1

1. Introduction and Problem Statement

A mobile ad-hoc network (MANET) is a wireless network with no fixed infrastructure and no central administration. Nodes have to cooperate to route the packets from source node to destination node. Every node may function as both a data source and a router that forward data for other nodes. Routing protocols are essential for a MANET in order to discover network topology and build routes, MANET routing protocols are designed to dynamically maintain routes between any pair of communicating nodes in spite of frequent topology changes caused by nodes' mobility. A lot of routing protocols have been proposed in the literature [1], including proactive, reactive, and hybrid solutions. Broch et al. [2] gives a simulation study of MANET routing protocols on different mobility and traffic scenarios. However, the absence of any trusted third party in such networks may result in nodes deviating from the routing protocol for selfish or malicious reasons. For example a selfish user may wish to preserve energy resources, while a malicious user might attempt a denial of service attack.

Security is an essential service for wired and wireless network communications [3]. The success of mobile ad hoc networks (MANET) strongly depends on people's confidence in its security. However, the characteristics of MANET pose both challenges and opportunities in achieving security goals, such as confidentiality, authentication, integrity, availability, access control, and non-repudiation.

The components of MANETs are mostly battery operated devices. The battery lifetime is one of the central issues. As each node acts as both host and router of packets, the battery

of the host runs down very quickly if high traffic is routed through it, leading to non functioning of the node and hence the broken link in the network. In an infrastructure network, the existence of the central base station allows the hosts to carryout calculations requiring high CPU power and memory to be done at the high power base station. Non —→

Existence of the Central Base station in Ad hoc Networks means that the computations should be carried out locally by the hosts which highly Limits the Battery Lifetime. As the Battery Lifetime cannot be significantly improved, there is a need for designing energy-efficient software and hardware which minimizes the battery usage.

Trusted routing protocols are a new class of routing protocols in which routing decisions are made according to the trust model. The concept of “Trust” originally derives from the social sciences and is defined as the degree of subjective belief about the behaviors of a particular entity. Blaze et al. [4] first introduced the term “Trust Management” and identified it as a separate component of security services in networks. Trust management in MANETs is needed when participating nodes, without any previous interactions, must establish a network with an acceptable level of trust relationships among themselves.

Although a lot of research has been done in the area of routing for MANETs, the available routing mechanisms are not sufficient in the following aspects: From the application point of view, the performance is still far from what is achieved in fixed networks [17]. From the algorithmic point of view, they require information about the context of the single network node within routing algorithms [15]. Furthermore, routing protocols should consider energy constraints, security constraint (e.g. don't route through an insecure area) and in some applications, real-time constraints (delivery in time).

In order to attain maximum performance from the given ad hoc network, there is a high need to design the algorithms which take multiple factors like energy, trust etc., into consideration while taking the routing decision to forward the packets through intermediate routes.

Thus it is highly essential to take routing decisions which are based on remaining battery energy for long network lifetime and trust value for secure routing in malicious environment. This dissertation work addresses both these problems in MANETs by proposing a new robust trust mechanism against route misbehavior attacks over energy efficient AODV routing and its performance has been studied on simulated environment using JiST-SWANS.

1.1 Motivation

MANETs being infrastructure-less, mobile, wireless, battery dependant pose many technical challenges which require thorough understanding. Major Technical challenges[5] include Mobility, Scalability, Bandwidth Constraint, RF connectivity, Energy Constraints, Routing Fairness, Distributed Information Processing, Security etc.,

Ad hoc Routing algorithms must also implement fairness in order to prevent early partitioning of the ad hoc network into disjoint network segments. Without some form of network-level or link-layer security, a routing protocol for these networks is vulnerable to many forms of attacks [6]. It may be relatively simple to snoop network traffic, replay transmissions, manipulate packet headers, and redirect routing messages, within a wireless network without appropriate security measures. While these concerns exist within wired infrastructures and routing protocols as well, maintaining the "physical" security of the transmission media is harder in practice with MANETs.

Trust management is much more challenging in a MANET than in traditional centralized environments. For example, collecting trust information or evidence to evaluate trustworthiness is difficult due to mobility induced changes in network topology. Resource constraints further confine the trust evaluation process to only local information, so that trust establishment would be based on incomplete and incorrect information. The dynamic nature and characteristics of MANETs result in uncertainty

and incompleteness of the trust evidence that is continuously changing over time. These observations have motivated to build a Robust Trust Model to handle the problems that selfish and malicious nodes cause to the network, effectively and efficiently.

1.2 Problem Statement

The main objective of the present research work can be briefly stated as follows.

“To design a new robust secure trust model against various route misbehavior attacks that hamper the network performance, by developing a modified version of standard AODV protocol in which the routing decisions of nodes are taken based on the amount of trust present in the neighboring node through which the route request has to be routed and also the remaining battery energy of that node.”

In order to achieve this main objective, several sub objectives have been set to fulfill. The brief description of sub objectives has been as follows.

- To identify, define and design various types of route misbehavior attacks on a mobile ad hoc network.
- To design an efficient energy model to be followed by the batteries of network nodes, while discharging themselves by transmitting and receiving network packets.
- To develop a basic trust model which improves the network performance even under the presence of attacks.
- To extend the basic model by incorporating energy efficient routing decision mechanism which boosts up the network performance which is suffering with the presence of fatal attacks.

- To construct a network over which various modified version of the standard AODV needs to be tested for performance comparisons.

In order to achieve various sub objectives given earlier, we have taken the Ad hoc On Demand Distance Vector (AODV) protocol as our base protocol and all the study has been carried out over this reactive routing protocol.

1.3 Organization of report

Chapter 2 discusses with the working details of the AODV protocol and with the various design issues which make basic protocol vulnerable. In this chapter, the metrics for Energy Aware Routing have been discussed in detail and the working of energy aware routing over AODV protocol has been discussed. Also, the Notion of Trust has been introduced and a detail explanation has been given on how the traditional trust system differs in its characteristics compared to a reputation system. A detailed survey of various existing trust models has also been given.

Chapter 3 gives the detailed insight into the design details of the proposed trust model mechanism against various route misbehavior attacks present in the network. Here the type of attacks chosen for network analysis, the energy model followed to design the energy efficient routing methodology and the proposed framework has been explained clearly.

In Chapter 4, details of the network simulator i.e., JiST-SWANS architecture, used for network analysis have been concentrated along with the various parameters used in the establishing of a sample mobile network for validating the proposed framework.

Chapter 5 gives the in depth analysis of the results obtained from simulation using JiST-Swans network simulator.

Chapter 6 concludes the dissertation work giving specific directions for the future work on the proposed methodology.

At the end, we provide the referred papers and articles, and also provide the details about the papers published on related dissertation work.

2. Background and Literature Review

There are two major classes of routing protocols for MANETs: proactive and reactive protocols. In proactive protocols nodes devote resources to tracking routes in a routing table, whereas in reactive protocols, routes are discovered when needed to preserve node's resources. There is no existence of the Routing Tables in the reactive protocols in contrast to proactive protocols which maintain Routing Tables which are needed to be updated every time when the Network Topology changes in the MANET. In this thesis, we focus on the AODV reactive protocol and its variants as it is an efficient low-overhead approach.

2.1 Ad Hoc On-demand Distance Vector Routing and its Energy Issues

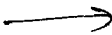
2.1.1 Overview of the Ad Hoc On-demand Distance Vector (AODV) Protocol

AODV is one of the reactive routing protocols developed for MANET. AODV builds routing tables on demand. When a source node needs to establish a route to a destination node, it broadcasts a route request message (RREQ) to all its neighbors. Each intermediate node receiving a RREQ message checks its routing table for the requested route. If a valid route is found, a route reply message (RREP) will be unicast back to the node initiating the route request, otherwise RREQ message will be broadcasted further until it reaches the destination. The destination, on its turn, unicasts a RREP to the source node. As the RREP message propagates back to the source node the required route is set

up. To avoid loops in the route established by the AODV, destination sequence numbers are introduced. Sequence numbers are used to identify the freshness of routes. Sequence numbers are carried in both the RREQ and RREP messages, and are incremented each time a mobile node sends a RREQ or a RREP. The sequence number in a RREP message must be larger than or equal to the one carried in the corresponding RREQ message to avoid the source node to adopt a stale route. When the source node receives several RREP messages, it chooses the route in the RREP message with the largest sequence number. If all RREP messages have the same sequence number, the route with the smaller hop count will be chosen.

The major difference between AODV and Dynamic Source Routing (DSR) stems out from the fact that DSR uses source routing in which a data packet carries the complete path to be traversed. However, in AODV, the source node and the intermediate nodes store the next-hop information corresponding to each flow for data packet transmission. The major difference between AODV and other on-demand routing protocols is that it uses a *destination sequence number* (DestSeqNum) to determine an up-to-date path to the destination. A node updates its path information only if the *DestSeqNum* of the current packet received is greater than the last *DestSeqNum* stored at the node. Much of the complexity of the protocol is to lower the number of messages to conserve the capacity of the network. For example, each request for a route has a sequence number. Nodes use this sequence number so that they do not repeat route requests that they have already passed on. Another such feature is that the route requests have a "time to live" number that limits how many times they can be retransmitted. Another such feature is that if a route request fails, another route request may not be sent until twice as much time has passed as the timeout of the previous route request.

The advantage of AODV is that it creates no extra traffic for communication along existing links. Also, distance vector routing is simple, and doesn't require much memory or calculation. However AODV requires more time to establish a connection, and the initial communication to establish a route is heavier than some other approaches.

The main advantage of this protocol is that routes are established on demand and destination sequence numbers are used to find the latest route to the destination. The connection setup delay is lower. One of the disadvantages of this protocol is that intermediate nodes can lead to inconsistent routes if the source sequence number is very old and the intermediate nodes have a higher but not the latest destination sequence 

number, thereby having stale entries. Also multiple RouteReply packets in response to a single RouteRequest packet can lead to heavy control overhead. Another disadvantage of AODV is that the periodic beaconing leads to unnecessary bandwidth consumption.

➤ **Security in MANETs**

One of the fundamental vulnerabilities of MANETs comes from their open peer-to-peer architecture. Unlike wired networks that have dedicated routers, each mobile node in an ad hoc network may function as a router and forward packets for other nodes. The wireless channel is accessible to both legitimate network users and malicious attackers. As a result, there is no clear line of defense in MANETs from the security design perspective. There is no well-defined place or infrastructure where we may deploy a single security solution. Attackers may sneak into the network through these subverted nodes, which pose the weakest link and incur a domino effect of security breaches in the system. We shall see the implementation and their impact of two such attacks namely Blackhole Attack and GreyHole Attacks in this project.

➤ **Attacks on MANETs**

There are a wide variety of attacks that target the weakness of MANET. For example, routing messages are an essential component of mobile network communications, as each packet needs to be passed quickly through intermediate nodes, which the packet must traverse from a source to the destination. Malicious routing attacks can target the routing discovery or maintenance phase by not following the specifications of the routing protocols. There are also attacks that target some particular routing protocols, such as

DSR, or AODV. More sophisticated and subtle routing attacks have been identified in recent published papers, such as the blackhole (or sinkhole) [8], Byzantine [9], and wormhole [10] attacks. Currently routing security is one of the hottest research areas in MANET.

2.1.2 Metrics for Energy Aware Routing

The first generation of routing protocols in ad hoc networks are essentially minimum hop routing protocols (MHRP) that do not consider energy efficiency as the main goal. While energy conservation becomes a major concern for the ad hoc network, many energy-aware routing algorithms have been proposed in recent years.

Singh et al. [11] propose several metrics for energy-aware routing:

- *Minimize Energy Consumed/Packet.* In this way, the total energy consumption of this network is minimized. However, it may cause some nodes to drain energy out faster since it tends to route packet around areas of congestion in the network.
- *Maximize Time to Network Partition.* Given a network topology, there exists a minimal set of nodes, the removal of which will cause the network to partition. The routes between these two partitions must go through one of these critical nodes. A routing procedure therefore must divide traffic among these nodes to maximize the lifetime of the network.
- *Minimize Variance in Node Power Levels.* The intuition behind this metric is that all nodes in the ad hoc network are of equal importance, and no node must be penalized more than any other nodes. This metric ensures that all the nodes in the network remain up and running together.
- *Minimize Cost/Packet.* In order to maximize the lifetime of all nodes in the network, metrics other than energy consumed/packet need to be used. The paths selected when using these metrics should be such that nodes with depleted energy reserves do not lie on many paths.

- *Minimize Maximum Node Cost.* This metric ensures that node failure is delayed. Unfortunately, there is no way to implement this metric directly in a routing protocol. However, minimizing the cost/node does significantly reduces the maximum node cost in the network.

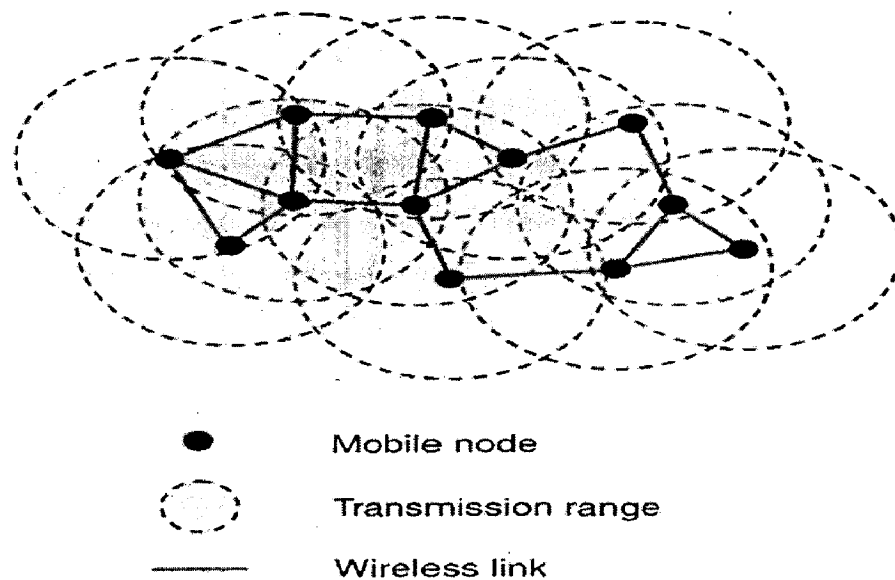


Figure 2.1: Generalized MANET Topology

2.1.3 Energy-Aware Routing Based on AODV

The main objective in Energy-Aware Routing (EAR)-AODV is to balance energy consumption among all participating nodes for an ad hoc topology as shown in Figure 2.1. In this approach, each mobile node relies on local information about the remaining battery level to decide whether to participate in the selection process of a routing path or not. An energy-hungry node can conserve its battery power by not forwarding data packets on behalf of others. The decision-making process in EAR-AODV is distributed to

all relevant nodes. Route discovery and route maintenance for EAR-AODV are described below.

➤ **Route discovery**

In AODV, each mobile node has no choice and must forward packets for other nodes. In EAR-AODV, each node determines whether or not to accept and forward the RREQ message depending on its remaining battery power (E_r). When it is lower than a threshold value (Th) the RREQ is dropped ($E_r < Th$); otherwise, the message is forwarded. The destination will receive a route request message only when all intermediate nodes along the route have enough battery levels.

➤ **Route maintenance**

Route maintenance is needed either when the connections between some nodes on the path are lost due to node mobility, or when the energy resources of some nodes on the path are depleting too quickly. In the first case, and as in AODV, a new RREQ is sent out, and the entry in the route table corresponding to the node that has moved out of range is removed. In the second case, the node sends an RERR back to the source even when the condition ($E_r \leq Th$) is satisfied. This route error message forces the source to initiate route discovery again. This is a local decision because it is dependent only on the remaining battery capacity of the current node. However, if this decision is made for every possible route, the source will not receive an RREP message even if a route exists between the source and the destination.

To avoid this situation, the source will resend another RREQ message with an increased sequence number. When an intermediate node receives this new request, it lowers its Th by d to allow the packet forwarding to continue. We use a new control message, *CHANGE_Thr*. When a node drops an RREQ message, it instead broadcasts a *CHANGE_Thr* message. The subsequent nodes closer to the destination now know that a request message was dropped and lower their threshold values. Now, the second route request message can reach the destination. When the destination receives an RREQ, it

generates an RREP. As in AODV, the RREP is routed back to the source via the reverse path.

2.1.4 Power Conserving Methods at Various Layers of Protocol Stack

Due to the success of the layered architecture of current Internet, wireless ad hoc networks are also developed based on the same layered structure with slight modifications. The Power Management at various Layers of the Protocol stack has been given in Table 1.

Protocol Layer	Methods to Conserve Power
Data-Link Layer	Turn radio off (sleep) when not transmitting or receiving. Avoid unnecessary retransmission. Avoid collision in channel access whenever possible. Put receive in standby mode whenever possible. Use or allocate contiguous slots for transmission and reception whenever possible.
Network Layer	Consider battery life in route selection. Reduce frequency of sending control message. Optimize size of control headers. Efficient route reconfiguration techniques. Consider route relaying load.
Transport Layer	Use power-efficient error control schemes. Avoid repeated retransmissions. Handle packet loss in a localized manner.

Table 2.1: Methods to Conserve Power at Various Protocol Layers

2.2 Background for Trust Based Systems

2.2.1 The Notion of Trust

Manifestations of trust are easy to recognize because we experience and rely on it every day, but at the same time trust is quite challenging to define because it manifests itself in many different forms. The literature on trust can also be quite confusing because the term is being used with a variety of meanings [12]. Two common definitions of trust which we will call reliability trust and decision trust respectively will be used in this study.

As the name suggest, reliability trust can be interpreted as the reliability of something or somebody, and the definition by Gambetta [13] provides an example of how this can be formulated:

Definition 1 (Reliability Trust) Trust is the subjective probability by which an individual, A, expects that another individual, B, performs a given action on which its welfare depends.

This definition includes the concept of dependence on the trusted party, and the reliability (probability) of the trusted party, as seen by the trusting party. However, trust can be more complex than Gambetta's definition indicates. For example, Falcone & Castelfranchi [14] recognise that having high (reliability) trust in a person in general is not necessarily enough to decide to enter into a situation of dependence on that person. In order to capture this broad concept of trust, the following definition inspired by McKnight & Chervany [15] can be used.

Definition 2 (Decision Trust) Trust is the extent to which one party is willing to depend on something or somebody in a given situation with a feeling of relative security, even though negative consequences are possible.

The relative vagueness of this definition is useful because it makes it the more general. It explicitly and implicitly includes aspects of a broad notion of trust which are *dependence* on the trusted entity or party, the *reliability* of the trusted entity or party, *utility* in the

sense that positive utility will result from a positive outcome, and negative utility will result from a negative outcome, and finally a certain *risk attitude* in the sense that the trusting party is willing to accept the situational risk resulting from the previous elements. Risk emerges, for example, when the value at stake in a transaction is high, and the probability of failure is non-negligible (i.e. reliability < 1). Contextual aspects, such law enforcement, insurance and other remedies in case something goes wrong, are only implicitly included in the definition of trust above, but should nevertheless be considered to be part of trust.

There are only a few computational trust models that explicitly take risk into account [16]. Studies that combine risk and trust include Manchala [17] and Jøsang & Lo Presti [18]. Manchala explicitly avoids expressing measures of trust directly, and instead develops a model around other elements such as transaction values and the transaction history of the trusted party. Jøsang & Lo Presti distinguish between reliability trust and decision trust, and develops a mathematical model for decision trust based on more finely grained primitives, such as agent reliability, utility values, and the risk attitude of the trusting agent.

Definition 3 (Reputation) Reputation is what is generally said or believed about a person's or thing's character or standing.

This definition corresponds that reputation is a quantity derived from the underlying social network which is globally visible to all members of the network. The difference between trust and reputation can be illustrated by the following perfectly normal and plausible statements:

- (1) "I trust you because of your good reputation."
- (2) "I trust you despite your bad reputation."

Assuming that the two sentences relate to identical transactions, statement (1) reflects that the relying party is aware of the trustee's reputation, and bases his trust on that.

Statement (2) reflects that the relying party has some private knowledge about the trustee, e.g. through direct experience or intimate relationship, and that these factors overrule any reputation that a person might have. This observation reflects that trust ultimately is a personal and subjective phenomenon that is based on various factors or evidence, and that some of those carry more weight than others. Personal experience typically carries more weight than second hand trust referrals or reputation, but in the absence of personal experience, trust often has to be based on referrals from others. Reputation can be considered as a collective measure of trustworthiness (in the sense of reliability) based on the referrals or ratings from members in a community.

An individual's subjective trust can be derived from a combination of received referrals and personal experience. In order to avoid dependence and loops it is required that referrals be based on firsthand experience only, and not on other referrals.

As a consequence, an individual should only give subjective trust referral when it is based on first hand evidence or when second hand input has been removed from its derivation base [19]. It is possible to abandon this principle for example when the weight of the trust referral is normalized or divided by the total number of referrals given by a single entity.

2.2.2 Difference between a Trust System and a Reputation System

Reputation can relate to a group or to an individual. A group's reputation can for example be modeled as the average of all its members' individual reputations, or as the average of how the group is perceived as a whole by external parties. Tadelis' [20] study shows that an individual belonging to a given group will inherit an *a priori* reputation based on that group's reputation. If the group is reputable all its individual members will *a priori* be perceived as reputable and vice versa.

According to Resnick et al. [21], reputation systems must have the following three properties to operate at all:

1. Entities must be long lived, so that with every interaction there is always an expectation of future interactions.
2. Ratings about current interactions are captured and distributed.
3. Ratings about past interactions must guide decisions about current interactions.

The longevity of agents means, for example, that it should be impossible or difficult for an agent to change identity or pseudonym for the purpose of erasing the connection to its past behavior. The second property depends on the protocol with which ratings are provided, and this is usually not a problem for centralized systems, but represents a major challenge for distributed systems. The second property also depends on the willingness of participants to provide ratings, for which there must be some form of incentive. The third property depends on the usability of reputation system, and how people and systems respond to it. The basic principles of reputation systems are relatively easy to describe. However, because the notion of trust itself is vague, what constitutes a trust system is difficult to describe concisely. A method for deriving trust from a transitive trust path is an element which is normally found in trust systems. The idea behind trust transitivity is that when Alice trusts Bob, and Bob trusts Claire, and Bob refers Claire to Alice, then Alice can derive a measure of trust in Claire based on Bob's referral combined with her trust in Bob. This is illustrated in Fig.2.2 below.

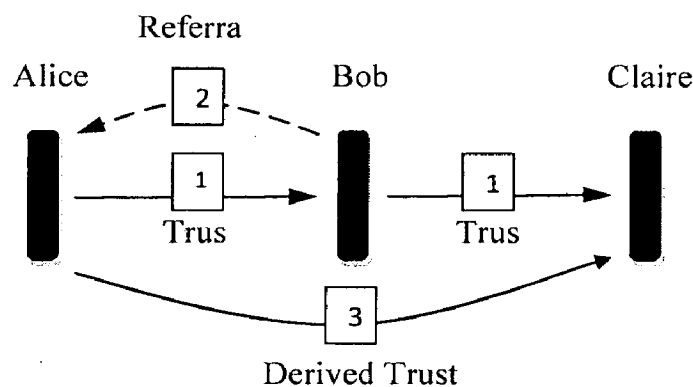


Figure 2.2: Trust transitivity principle

The type of trust considered in this example is obviously reliability trust (and not decision trust). In addition there are semantic constraints for the transitive trust derivation to be valid, i.e. that Alice must trust Bob to recommend Claire for a particular purpose, and that Bob must trust Claire for that same purpose.

The main differences between trust and reputation systems can be described as follows: Trust systems produce a score that reflects the relying party's subjective view of an entity's trustworthiness, whereas reputation systems produce an entity's (public) reputation score as seen by the whole community. Secondly, transitivity is an explicit component in trust systems, whereas reputation systems usually only take transitivity implicitly into account. Finally, trust systems usually take subjective and general measures of (reliability) trust as input, whereas information or ratings about specific (and objective) events, such as transactions, are used as input in reputation systems.

2.2.3 Survey of Various Existing Trust Models

Li et al. [22] classify trust management as reputation-based framework and trust establishment framework. A reputation-based framework uses direct observation and second-hand information distributed among a network to evaluate other nodes. A trust establishment framework evaluates neighboring nodes based on direct observations while trust relations between two nodes with no prior direct interactions are built through a combination of opinions from intermediate nodes.

The first secure routing based on Trust Management in MANETs is targeted at various malicious packet forwarding attacks[23]. This is an extension of DSR algorithm for Routing. Paul et al.[24] built a reputation based Trust Model targeting packet modification and masquerading attacks. This is also an extension of DSR routing algorithm, however, No experimental results have been showed[25]. Trust against False recommendation attacks and Newcomer attacks have been discussed in detail by Sun et al[26]. The methodology used is the direct observation on packet dropping rate at

malicious nodes in the network and the trust model proposed is a Probability based trust model. However authors suggest that higher mobility of the nodes can lead to higher false alarm rates when the detection rate is fixed with this approach.

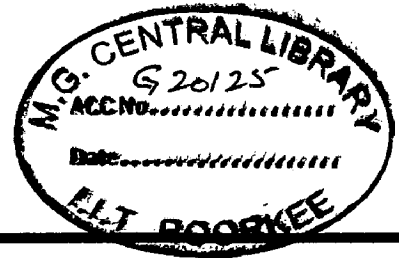
Golbeck [27] discusses the three main properties of trust in the context of a social network perspective: transitivity, asymmetry, and personalization. First, trust is not perfectly transitive in a mathematical sense. That is, if A trusts B , and B trusts C , it does not guarantee that A trusts C . Second, trust is not necessarily symmetric, meaning not identical in both directions. Third, trust is inherently a personal opinion. Two people often evaluate trustworthiness about the same entity differently.

Jiang and Baras [28] proposed a trust distribution scheme called ABED (Ant-Based trust Evidence Distribution) based on the swarm intelligence paradigm, which is claimed to be highly distributed and adaptive to mobility. The key principle is called stigmergy, indirect communication through the environment. In ABED, nodes interact with each other through “agents” called “ants” that deposit information called “pheromones”; based on this the agents can identify an optimal path for accumulating trust evidence. However, no specific attacks were considered in [28].

Theodorakopoulos and Baras [29] proposed a trust evidence evaluation scheme for MANETs. The evaluation process is modeled as a path problem in a directed graph where nodes indicate entities and edges represent trust relations. However, their work assumes that trust is transitive. Further, trust and confidence values are represented as binary rather than as a continuous-valued variable.

Recently Buckerche and Ren [30] proposed a distributed reputation evaluation prototype called GRE (Generalized Reputation Evaluation) to effectively prevent malicious nodes from entering the trusted community. However, no specific attack model was addressed. Further, transitivity, asymmetry, and subjectivity characteristics of trust concept were not specifically explained in building their trust model.

3. Design Details of Proposed Trust Model



3.1 Overall Design Strategy

In formulating the overall design strategy, in order to test the behavior of the network in the presence of malicious nodes and to observe how the trust model reduces the effect of these malicious nodes, two types of Route Misbehavior attacks namely Blackhole and Greyhole Attacks have been chosen. These attacks have been implemented over AODV as the base protocol on JIST-SWANS network simulator and the performance of the network following AODV routing, under the influence of these attacks have been studied. Later, a robust trust model has been devised which also consider the remaining battery power of the intermediate node into consideration along with the trust in the node and is implemented on the attacked network. The packet throughput of the network has been considered to evaluate the performance of the network at various stages of simulation work. The detailed explanation of various building blocks involved in the overall design of the system is as follows and is also depicted pictorially in the Figure 3.1.

➤ Selection of Specific Attacks on MANETs

Attacks can be classified broadly as *insider attack* versus *outsider attack*. If an entity is authorized to access system resources but employs them in a malicious way, it is classified as an *insider attack*. On the other hand, an *outsider attack* is initiated from unauthorized or illegitimate user from the system. Several Attacks like Routing Loop attack, Wormhole attack, Black hole attack, Grey Hole Attack, Denial-of-Service (DoS) attack etc., are possible on the MANETs. Among these, Black Hole Attack and Grey

Hole Attacks have been selected for the analysis of the network under the presence of the malicious behavior.

➤ **Design of Selected Attack Modules**

Three Different Attack Modules[31] namely Blackhole on Route Attack, Blackhole Fake Destination Reply Attack and Greyhole Attack have been designed and implemented in JiST- SWANS network simulator. The MANETs performance in the presence of these attacks is estimated and is compared for each of these different attacks.

➤ **Analysis of Network Performance in the presence of Different Attacks**

The Packet Throughput of the network has been considered to evaluate the effect of discussed attack models on AODV. Packet Throughput can be defined as the ratio of packets received by the destination to the number of packets sent (%). For AODV, increasing the number of malicious nodes very soon reduces throughput of the network. The degradation is more severe in the case of Blackhole FakeDestReply attack as the malicious node embeds the information of false route to the destination in the RREP message every time it receives the RREQ messages from its neighbors, which is unicasted to the source node.

➤ **Design of Secure Power Aware Trust Model against Attacks Specified**

A TrustNode data structure, which comprises a nodeID, a packetBuffer, an integer trustValue and batteryPower for the node has been introduced in the traditional AODV protocol. A PacketBuffer datastructure which is a circular buffer has been added for every node to store the sent packets information. The routing decision at the destination for RREP is taken based on the value of DecisonAvg which will be calculated for every route in all received RREQ messages. The implementation of the functioning of these data structures in the network with malicious nodes and the impact of the robust trust model in improving the throughput of the network effectively has been explained in

detail in the coming sections. The trust model is tested for accuracy with varying number of malicious nodes in the network and is validated by obtaining satisfactory results.

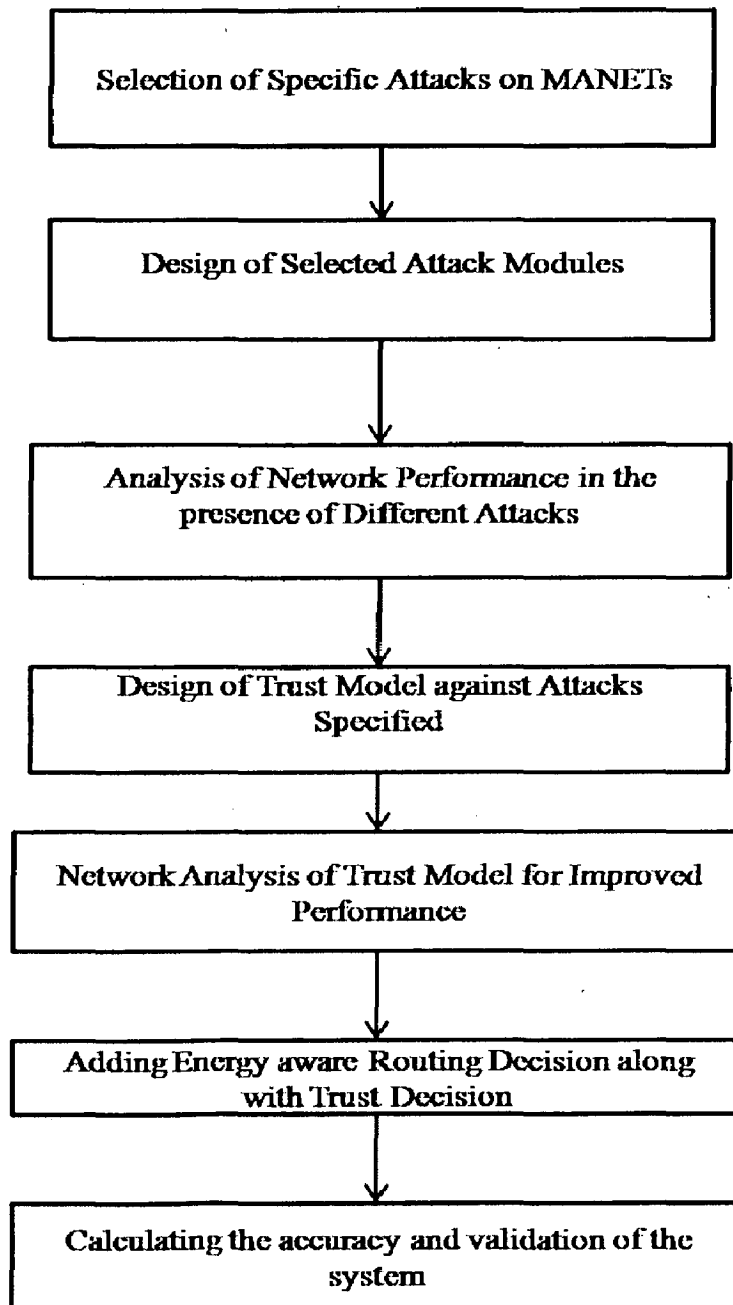


Figure 3.1: Overall Design Strategy for Robust Secure Trust Model.

3.2 Design of Attack Modules

The default AODV protocol without any improvisations considers that all the nodes in the network work properly and assumes the absence of any malicious or selfish nodes. However, if there are any malicious or selfish nodes in the network, the standard AODV does not cope up with the anomalous behavior of the network. In order to test the behavior of the network in the presence of malicious nodes and to observe how the trust model reduces the effect of these malicious nodes, two types of Route Misbehavior attacks namely Blackhole and Greyhole Attacks have been chosen. A blackhole is a malicious node that attempts to drop all packets, typically by forging route replies to create fake routes with it as an intermediate node. This allows the blackhole to divert and intercept traffic from across the network, and subsequently drop all packets that it receives. A greyhole can be viewed as a faulty node, rather than explicitly malicious. There are several possible mechanisms to implement these attacks within AODV, and we use the following definitions.

Blackhole on Route Attack

This operates by replying that it has a fresh enough route to the destination whenever it receives a RREQ, regardless of whether it actually knows a route. AODV uses sequence numbers to track the freshness of routes. When nodes issue a new RREQ or the destination responds the sequence number is increased. A Blackhole-OnRoute node claims to have an existing fresh route to the destination and so the generated RREP has the same sequence number as the RREQ, causing it to be accepted by the original sender, which subsequently creates a route with the blackhole as an intermediate node. This kind of a blackhole is partially guarded against within AODV, since if the original RREQ eventually reaches the intended destination a RREP will be generated. The reply from the destination itself has an increased sequence number over the RREQ and so will overwrite the malicious route setup by the blackhole. Despite this, in the simulations Blackhole-

OnRoute was able to cause significant packet loss, as the routes it created intercept the first packets sent across any new route until the destination's RREP was received.

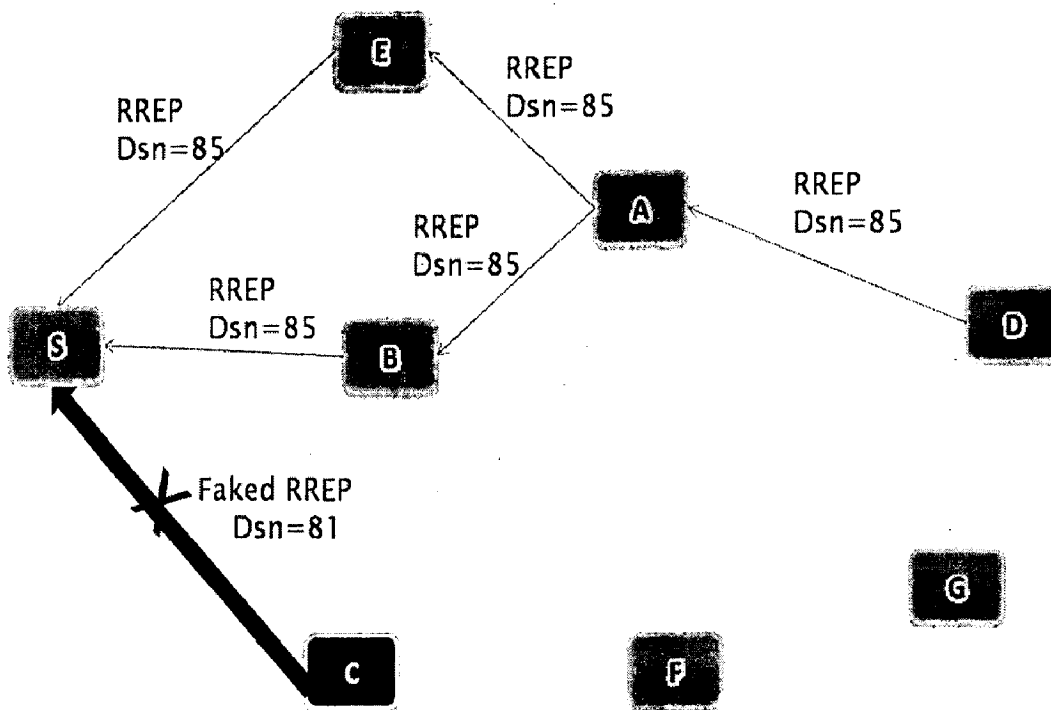


Figure 3.2: Working of Blackhole On Route Attack

Blackhole Fake Destination Reply Attack

This blackhole is more malicious than Blackhole-OnRoute, since in addition to claiming to have a recent enough route to the destination it also increases the sequence number in the RREP and so appears to offer a new route. The effect is that Blackhole-FakeDestReply's route is not overwritten by any reply subsequently returning from the destination itself. Thus, a route to the actual destination will only be established when the destination's RREP is received before that generated by the Blackhole-FakeDestReply node. The working

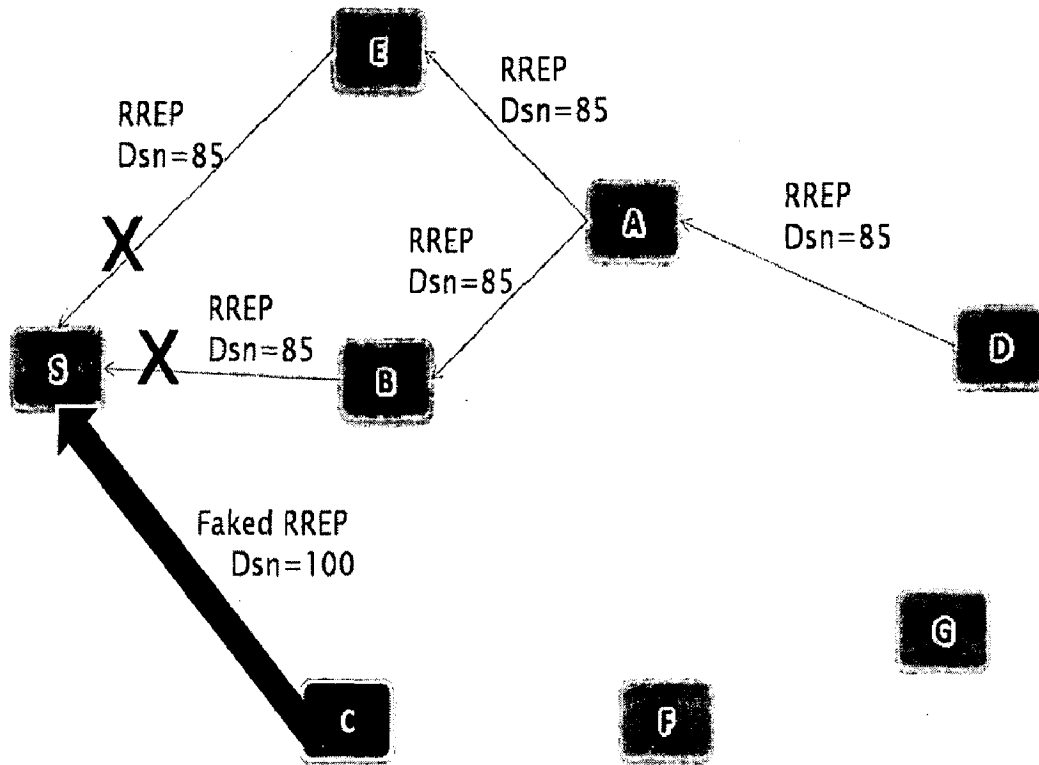


Figure 3.3: Working of Blackhole Fake Dest Reply Attack

Greyhole Attack

The Greyhole does not falsify route replies in order to intercept packets, but instead simulates a node having intermittent faults as shown in Figure 3.4. We characterise a Greyhole using two time periods:

- MAX_TIME_TO_BURST_FAULT: maximum time to the next burst fault (seconds)
- MAX_TIME_BURST_FAULT_LASTS: maximum burst fault duration (seconds)

Using these time periods a node will start a burst fault at a random time between 0 and MAX_TIME_TO_BURST_FAULT. The burst fault lasts for a random period between 0 and MAX_TIME_BURST_FAULT_LASTS. These parameters can be modified to alter the nature of the faults.

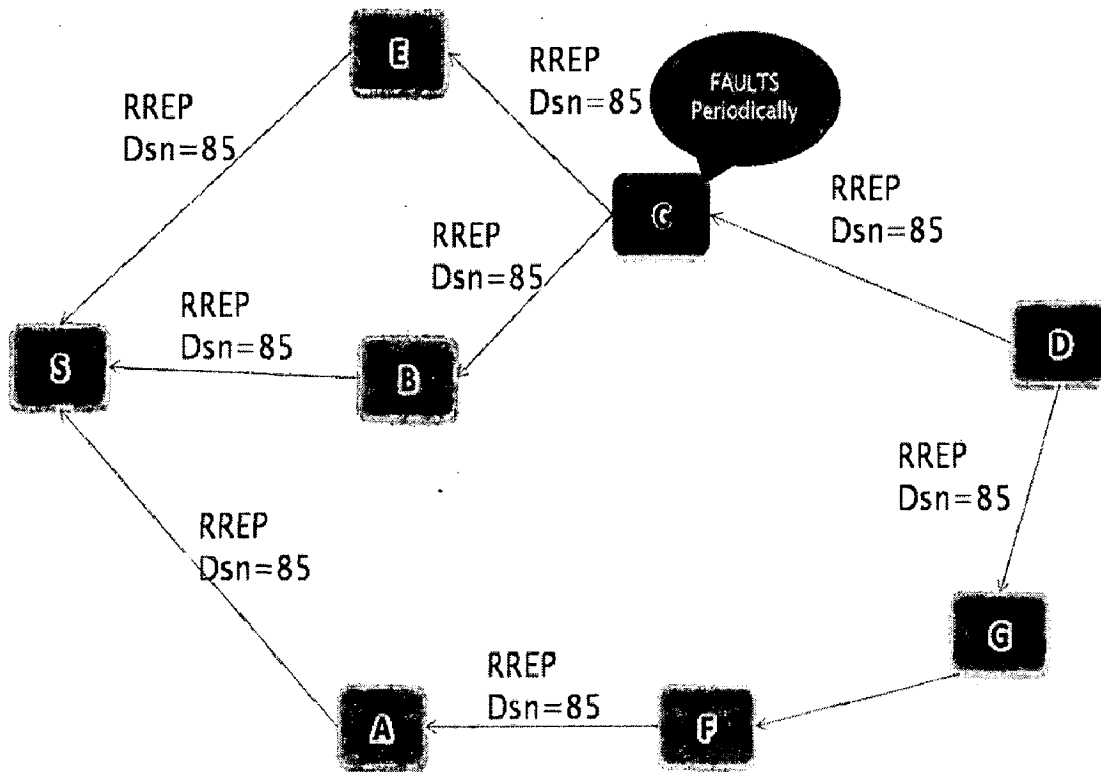


Figure 3.4: Working of GreyHole Attack

3.3 Design of Energy Model

Every node in network periodically calculates its energy consumed because of Transmission and Reception of Packets. For this purpose, a simple energy consumption model [32] has been chosen to evaluate the performance of trust mechanism on power aware AODV protocol. Energy consumption of a node after time t is calculated as

$$E_{\text{cons}}(t) = x * N_t + y * N_r \quad \text{----- (1)}$$

Where,

$E_{\text{cons}}(t)$ is the Energy consumed by node at time t

N_t is the Number of packets Transmitted by node after time t

N_r is the Number of packets Received by node after time t

x and y are constants such that $0 \leq x, y \leq 1$

The Total energy consumed is calculated independently [32] by taking into account the amount of energy spent on Transmission or Reception of packets as follows

In Transmission mode, the power consumed for transmitting a packet is given by the Eq (2)

$$\text{Consumed energy} = P_t * T \quad \text{----- (2)}$$

Where P_t is the transmitting power and T is transmission time.

In Reception mode, the power consumed for receiving a packet is given by Eq (3)

$$\text{Consumed energy} = P_r * T \quad \text{----- (3)}$$

Where P_r is the reception power and T is the reception time.

The value T can be calculated as

$$T = \text{Data size} / \text{Data rate} \quad \text{----- (4)}$$

Hence, the remaining energy of each node can be calculated using Eq (2) or Eq(3)

$$\text{Remaining energy } E_{\text{rem}} = \text{Current energy} - \text{Consumed energy} \quad \text{----- (5)}$$

Initially all the nodes are assigned with the maximum battery capacity. With each packet reception and transmission, the battery energy associated with the node decreases. If the residual energy associated with the node falls below the threshold value, the node stops functioning there by opting itself out of the routing process.

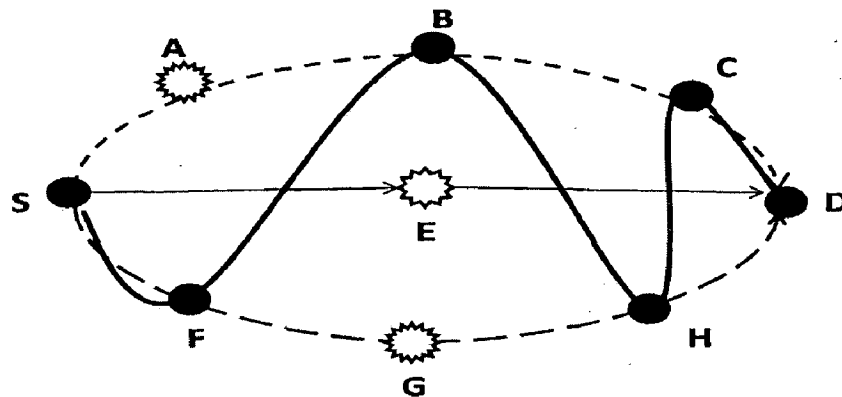
3.4 Proposed Framework for Robust Trust Mechanism

Trustworthiness of the nodes in the network has been calculated using the method of Passive Acknowledgement. Using Passive Acknowledgement, we make sure that the network works in promiscuous mode in order to monitor the channel [33]. The packets which are forwarded for the neighboring node will be observed if they are indeed forwarded by the node or not, irrespective of their actual destination in this mode. In computing, promiscuous mode or *promisc mode* is a configuration of a network card that makes the card pass all traffic it receives to the kernel rather than just frames addressed to it, a feature normally used for packet sniffing, and bridged networking for hardware virtualization. Each frame includes the hardware (Media Access Control) address. When a network card receives a frame, it normally drops it unless the frame is addressed to that card. In promiscuous mode, however, the card allows all frames through, thus allowing the computer to read frame intended for other machines or network devices [34].

Many operating systems require superuser privileges to enable promiscuous mode. A non-routing node in promiscuous mode can generally only monitor traffic to and from other nodes within the same collision domain (for Ethernet and Wireless LAN) or ring (for Token ring or FDDI). Computers attached to the same network hub satisfy this requirement, which is why network switches are used to combat malicious use of promiscuous mode. A router may monitor all traffic that it routes. Promiscuous mode is often used to diagnose network connectivity issues. There are programs that make use of this feature to show the user all the data being transferred over the network. Some protocols like FTP and Telnet transfer data and passwords in clear text, without encryption, and network scanners can see this data. Therefore, computer users are encouraged to stay away from insecure protocols like telnet and use more secure ones such as SSH. Promiscuous mode is also used by transparent network bridges in order to capture all traffic that needs to pass the bridge so that it can be retransmitted on the other side of the bridge. The selection of route is made as shown in Figure 3.5 by taking each of the features into consideration. The number of hops between source node and

destination node, the residual energy of the route and the amount of trust in the route are the three important factors taken into account while making a routing decision as shown. In the figure, the route S-F-B-H-C-D is the most efficient route off all available ones and will be chosen for routing data packets according to the proposed methodology.

For evaluating trust over power aware AODV protocol we take a data structure called GetTrust with the Fields of TrustPres, TrustThres, TrustLowest which will be maintained by all the nodes for each of their neighboring nodes. To detect whether a packet is successfully forwarded, the packets that have been recently sent for forwarding are stored in the packetBuff. This is a circular buffer, meaning that if packets are not removed



- S->Source Node, D -> Destination Node
- E,G -> Low Energy Nodes , A-> Blackhole Node
- S-E-D Shortest Route but not Energy Efficient
- S-A-B-C-D Non Trustable
- S-F-G-H-D Non Energy Efficient
- S-F-B-H-C-D Efficient and Trustable Route

Figure 3.5: Selection of Shortest, Most Trustable and Energy Efficient Route out of available routes

frequently enough the buffer will cycle, erasing the oldest elements. Thus, if a node is dropping packets or is being unacceptably slow at forwarding packets then the buffer will cycle as shown in the Figure 3.6.

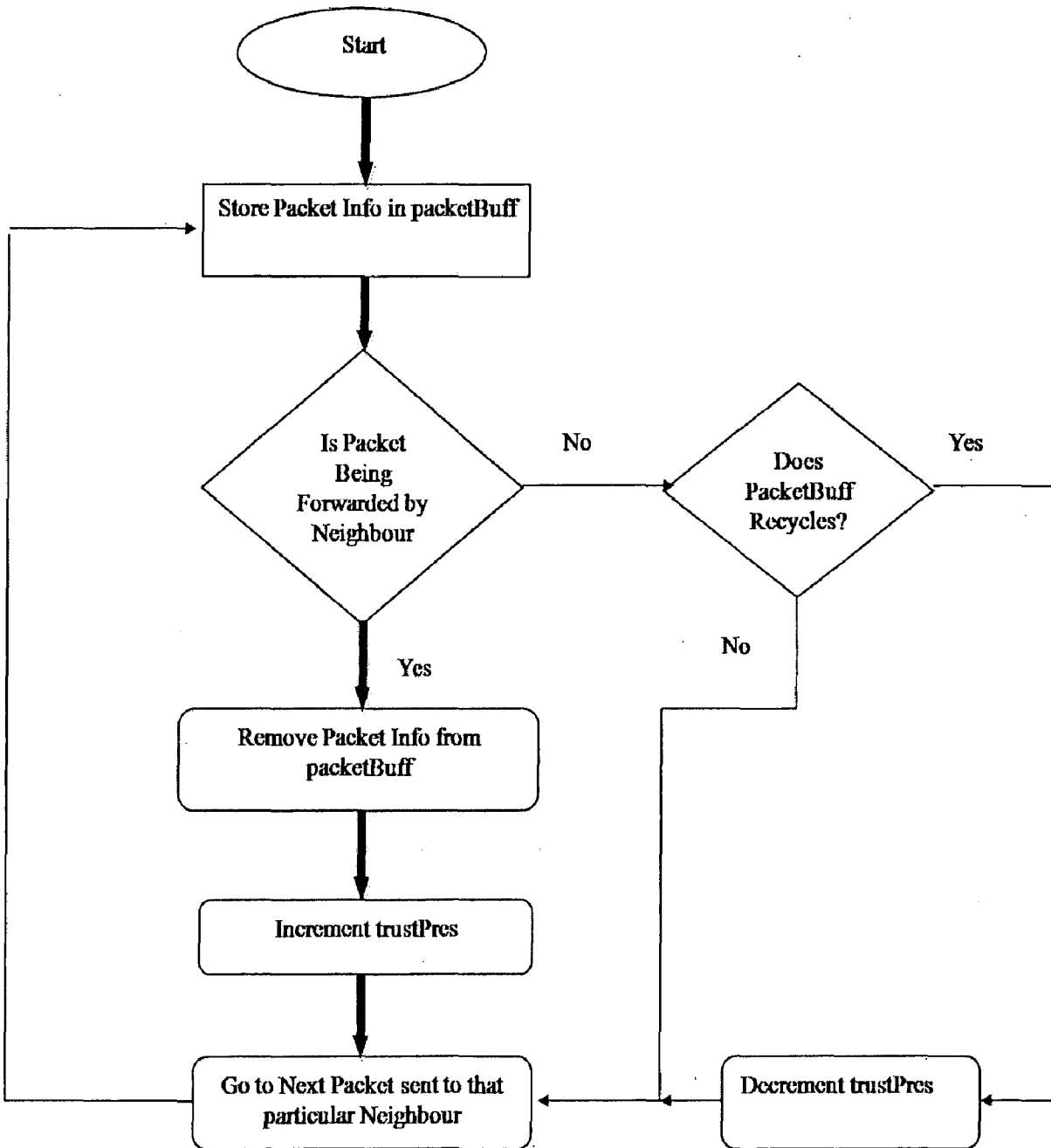


Figure 3.6: Working of packetBuff DataStore while Forwarding a Packet to the Neighbour

Initially, TrustPres for each node will be initiated to 0. If the node is detected to forward packets, TrustPres is incremented. If it is not forwarding or unacceptably slow, TrustPres value is Decrementated. We calculate the Residual Energy of each node E_{res} using the previous theory.

Now at each Intermediate Node, we first check for the TrustPres value of that node to be higher than the TrustThres. If so, it means that the node is trusted and can be used for forwarding packets. Then we check whether the Residual Energy of the neighboring node is higher than the Energy Threshold. If both these conditions are met, then only the RREQ is forwarded to the next neighboring node by updating TrustLowest and EnergyLowest Variables, else it is discarded as the node does not have enough energy reserves to forward the packets. This route decision methodology has been shown in the Figure 3.7.

At the destination, a timer is started when the first RREQ is received. After receiving all the RREQ till the timer expires, **TrustLowest** and **EnergyLowest** values in each RREQ are checked against the Thresholds. If both are above the respective thresholds, their average is calculated and stored in **DecisionAvg** of that RREQ. If any of the Thresholds is not satisfied, the RREQ is discarded. The Highest of these **DecisionAvg** values is chosen to be the desired route among the available routes and the RREP will be sent with the route as the Obtained route in RREQ with highest **DecisionAvg**. When receiving a RREP the first hop node is checked and if it is untrusted then the reply is disregarded. Thus, only routes where the first hop is trusted are established. This mechanism is explained diagrammatically in the Figure 3.8.

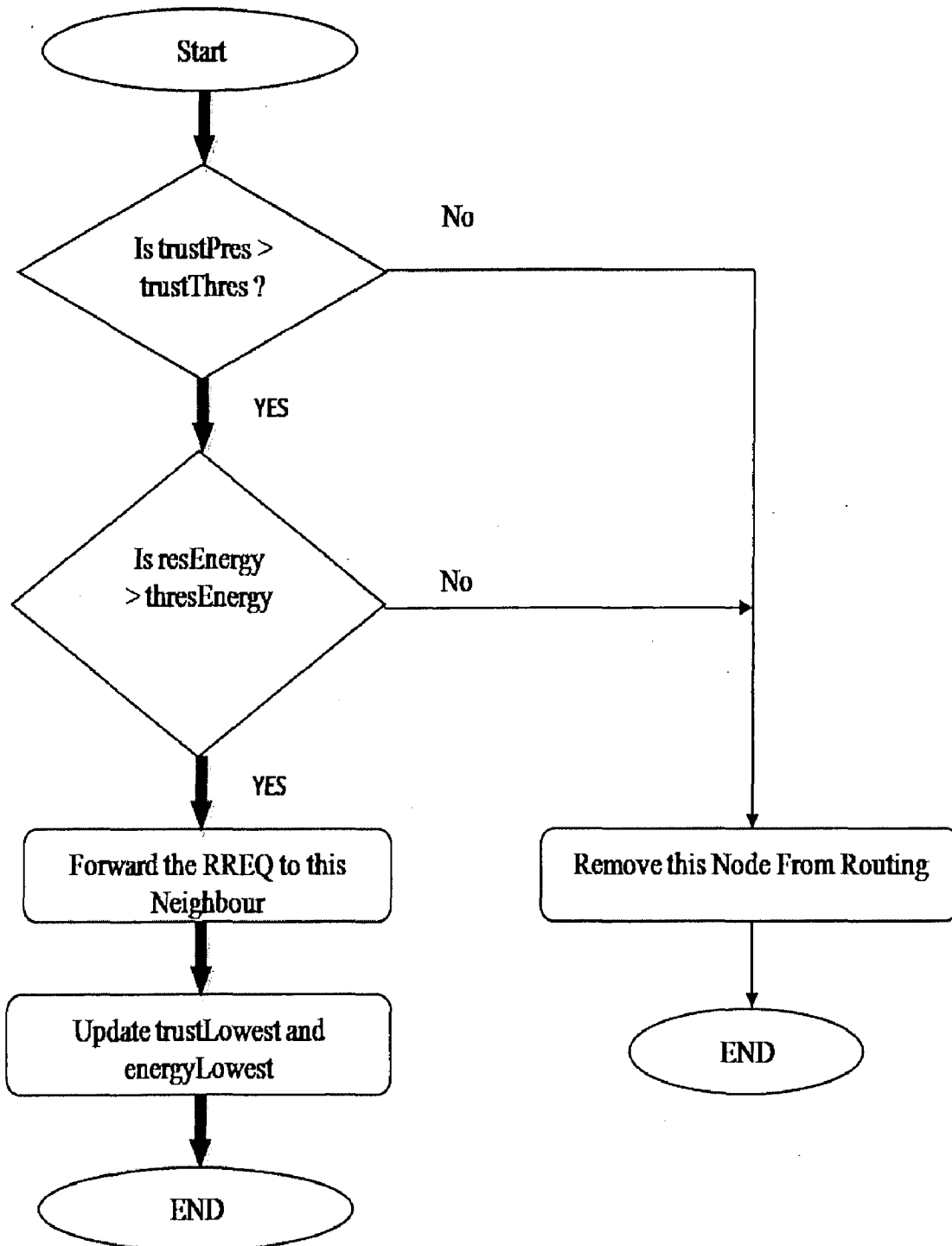


Figure 3.7: Routing Decision Methodology at Intermediate Nodes (Routers)

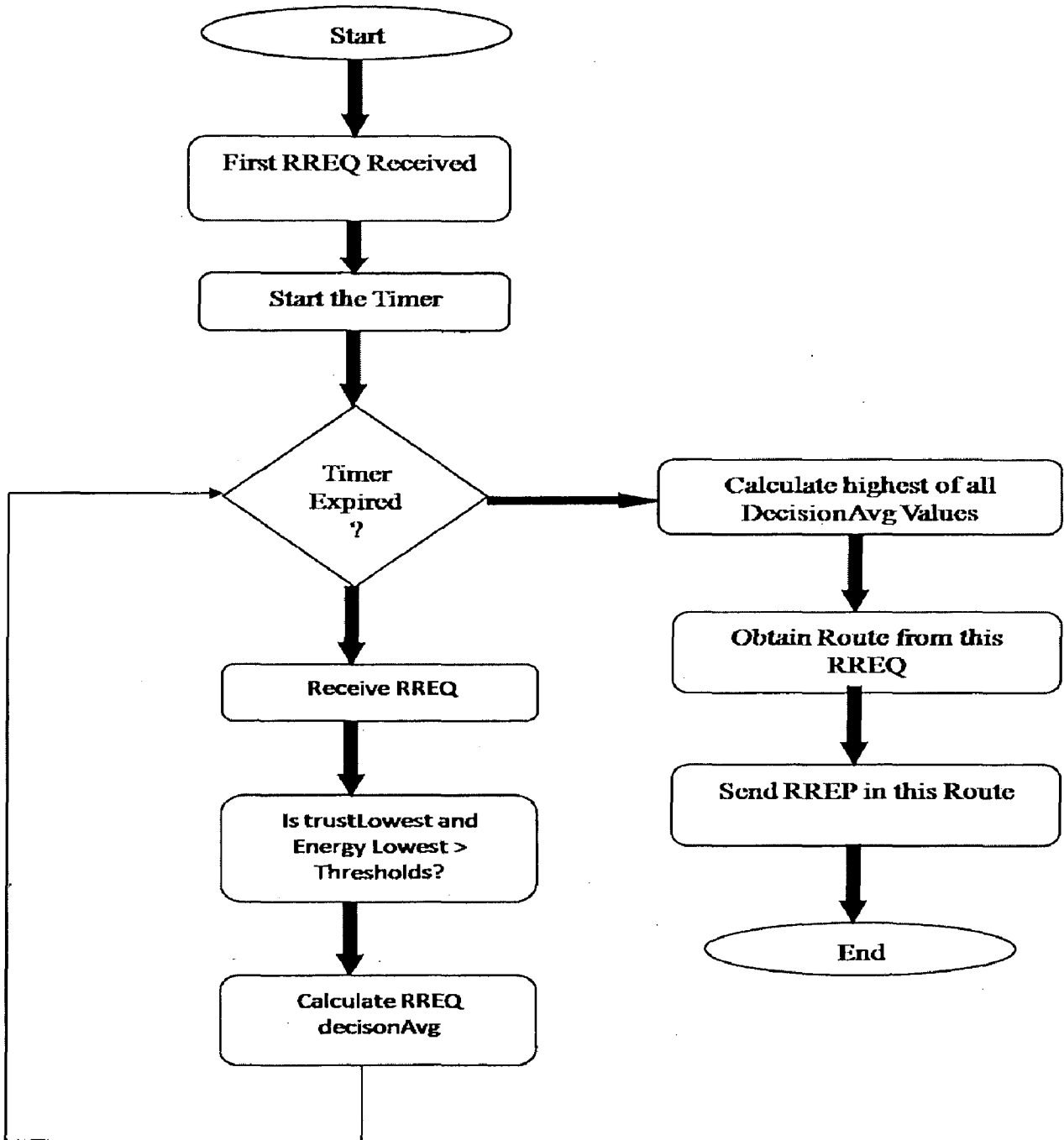


Figure 3.8: Route Selection Methodology among various available routes at the Destination Node

Once a node becomes untrusted or runs out of batteryPower, it is barred from consideration for packet forwarding by dropping it from the set of neighbours, removing all routes that use it, and sending out a new RREQ to re-establish the removed routes. Similarly, when receiving a RREP the first hop node is checked and if it is untrusted then the reply is disregarded. Thus, only routes where the first hop is trusted are established. Nodes make routing choices based on trust as well as the number of hops, such that the selected next hop gives the shortest trusted path.

4. Simulation and Implementation Details

4.1 Java in Simulation Time (JiST) Engine Architecture

The JiST system architecture consists of four distinct components: a compiler, a bytecode rewriter, a simulation kernel and a virtual machine. One writes JiST simulation programs in plain, unmodified Java and compiles them to bytecode using a regular Java language compiler. These compiled classes are then modified, via a bytecode-level rewriter, to run over a simulation kernel and to support the *simulation time* semantics described shortly. The simulation program, the rewriter and the JiST kernel are all written in pure Java. Thus, this entire process occurs within a standard, unmodified Java virtual machine (JVM).

The benefits of this approach to simulator construction over traditional systems and languages approaches are numerous. Embedding the simulation semantics within the Java language allows us to reuse a large body of work including the Java language itself, its standard libraries and existing compilers. JiST benefits from the automatic garbage collection, type-safety, reflection and many other properties of the Java language. This approach also lowers the learning curve for users and facilitates the reuse of code for building simulations. The use of a standard virtual machine provides an efficient, highly-optimized and portable execution platform and allows for important crosslayer optimization between the simulation kernel and running simulation. Furthermore, since the kernel and the simulation are both running within the same process space we reduce serialization and context switching overheads. In summary, a key benefit of the JiST approach is that it allows for the efficient execution of simulation programs within the context of a modern and popular language. JiST combines simulation semantics, found in

custom simulation languages and simulation libraries, with modern language capabilities. This design results in a system that is convenient to use, robust and efficient.

4.2 Scalable Wireless Ad hoc Network Simulator (SWANS)

The two most popular simulators in the wireless networking space are ns2 and GloMoSim. The ns2 network simulator [35] has a long history with the networking community, is widely trusted, and has been extended to support mobility and wireless networking protocols. It is built as a monolithic, sequential simulator, in the *library-systems* simulator design. ns2 uses a clever “split object” design, which allows Tcl-based script configuration of C-based object implementations. This approach is convenient for users. However, it incurs a substantial memory overhead and increases the complexity of simulation code. Researchers have extended ns2 to conservatively parallelize its event loop [36]. However, this technique has proved primarily beneficial for distributing ns2’s considerable memory requirements. Based on numerous published results, it is not easy to scale ns2 beyond a few hundred simulated nodes.

Simulation researchers have shown ns2 to scale, with difficulty and substantial hardware resources, to simulations of a few thousand nodes [37]. GloMoSim [38] is a newer simulator written in Parsec, a highly-optimized C-like simulation language. Glo-MoSim has recently gained popularity within the wireless ad hoc networking community. It was designed specifically for scalable simulation by explicitly supporting efficient, conservatively parallel execution with lookahead. The sequential version of GloMoSim is freely available. The conservatively parallel version has been commercialized as QualNet. Due to Parsec’s large per-entity memory requirements, GloMoSim implements a technique called “node aggregation,” wherein the state of multiple simulation nodes are multiplexed within a single Parsec entity. While this effectively reduces memory consumption, it incurs a performance overhead and also increases code complexity. The aggregation of state also renders speculative execution techniques impractical. GloMoSim has been shown to scale to 10,000 nodes on large, specialized multi-processor machines.

The SWANS simulator runs over JiST, combining the traditional systems-based (e.g., ns2) and languages-based (e.g., GloMoSim) approaches to simulation construction. SWANS is able to simulate much larger networks and has a number of other advantages over existing tools. The JiST design is leveraged within SWANS to:

(1) achieve high simulation throughput

Simulation events among the various entities, such as packet transmissions, are performed with no memory copy and no context switch. The system also continuously profiles running simulations and dynamically performs code inlining, constant propagation and other important optimizations, even across entity boundaries. This is important, because many stable simulation parameters are not known until the simulation is running. Greater than 10 speedups have been observed.

(2) save memory

Memory is critical for simulation scalability. Automatic garbage collection of events and entity state not only improves robustness of long-running simulations by preventing memory leaks, it also saves memory by facilitating more sophisticated memory protocols. For example, network packets are modeled as immutable objects, allowing a single copy to be shared across multiple nodes. This saves the memory (and time) of multiple packet copies on every transmission. A different example of memory savings in SWANS is the use of soft references for storing cached computations, such as routing tables. These routing tables can be automatically collected, as necessary, to free up memory.

(3) run standard Java applications

SWANS can run existing Java network applications, such as web servers and peer-to-peer applications, over the simulated network without modification. The application is automatically transformed to use simulated sockets and into a continuation-passing style. The original network applications are run within the

same process as SWANS, which increases scalability by eliminating the considerable overhead of process-based isolation.

In addition to the simulator design, it is also essential to model wireless signal propagation efficiently, since this computation is performed on every packet transmission. The hierarchical binning data structure allows node location updates in expected amortized constant time and receiver node set computations in time proportional to the number of receivers. The combination of these attributes leads to a flexible and efficient simulator.

SWANS is organized as independent software components that can be composed to form complete wireless network or sensor network configurations. Its capabilities are similar to ns2 and GloMoSim, but is able to simulate much larger networks. SWANS leverages the JiST design to achieve high simulation throughput, save memory, and *run standard Java network applications* over simulated networks. In addition, SWANS implements a data structure, called *hierarchical binning*, for efficient computation of signal propagation. Hierarchical binning of radios on the field allows location updates to be performed in expected amortized constant time and the set of receiving radios to be computed in time proportional to its size.

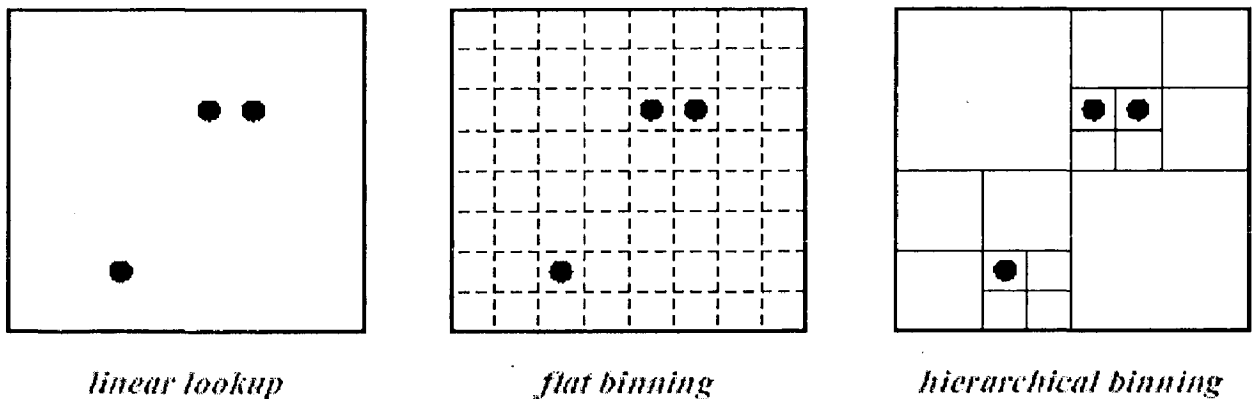


Figure 4.1: Alternative spatial data structures for radio signal propagation

SWANS is a complete library for simulation of MANETs running on the JiST engine. MANET simulations need a model for the environment and for the nodes. In SWANS, the Field entity provides node mobility and radio propagation. Nodes consist of a number of entities implementing various protocol layers, where the radio entity is connected to the global field entity. Packets traverse the protocol stack entities usually as simple references, at virtually no cost. Duplication is only done where necessary, e.g. if a packet is broadcasted and needs to be changed by the forwarders. Regarding radio propagation, one can choose a free space or a two-ray-ground pathloss model, together with Rayleigh fading, Rician fading or without fading. Moreover, a statistic packet dropping can be applied. As node mobility, the standard distribution supplies teleporting, random walk and random waypoint models. For the composition of nodes, SWANS brings basic radio noise models, an implementation of 802.11b MAC, IPv4, AODV, DSR and ZRP MANET routing, as well as TCP and UDP transport and several applications. As a special feature, SWANS also allows to run legacy Java network applications as part of simulations.

4.3 Simulation Set Up and Implementation

To evaluate the performance of Power-Aware Trusted AODV in the presence of route misbehavior attacks, a Java based network simulator namely JiST-SWANS is used. JiST is a high-performance discrete event simulation engine that runs over a standard Java virtual machine. SWANS is a scalable wireless network simulator built atop the JiST platform. The conventional code of AODV implemented in JiST has been modified in accordance with the attack models explained. Hence a new AODV for each of the three attacks have been designed.

Routing Protocol	AODV / Secure Trusted Power Aware AODV
No. of Network Nodes	50
No. Of Malicious Nodes	Varying
Simulation Area	1100x1100 sq.mtrs
Transmission Range	200m
Connection Type	CBR
Packet Size	512 Bytes
Node Speed	2-8 m/sec
Mobility Model	Random Waypoint
PathLoss Model	Two-Ray
Spatial Model	Hierarchical Grid
Placement	Random
Fading Model	Zero Fading Model
Antenna Gain	15dB
Interference Model	RadioNoiseAdditive

Table 4.1: Parameters Values used in Simulation

A new power-aware Trusted AODV is developed in order to test the performance of network in the presence of attacks. Malicious nodes in the network follow any one of the attack models designed and the remaining fair nodes follow the standard AODV protocol. A network of 50 nodes has been constructed in the driver to test the Attacks with the field possessing specifications in Table 4.1. Nodes move randomly with speeds varying from 2m/sec to 8m/sec. The simulation area is a 1100x1100 sq. meters with nodes randomly distributed all throughout the area. This setup matches a scenario of an open air, in which there are no obstacles from which the signal can reflect off and fade. The number of

malicious nodes is varied in the case of each of the attacks and the packets sent by the source node and those received by the destination are noted down.

Again a network of 1000 nodes has also been constructed with varying parameters and however minimal yet satisfactory performance improvement has been obtained. Various bugs present in the JiST SWANS free distribution software, have been fixed in order to improve the existing functionality of the simulator.

In order to implement Black Hole On Route Attack, AODV has been modified such that the routeToDestExists() and hasFreshRoute() methods always return TRUE irrespective of the route table entries for the required destination, so that the node pretends as if it has the fresh route to the Destination with hop count equal to 1. Hence the node will send the route reply to the source indicating a Fresh Route in the RREP message and drops forwarding the received RREQ packets. For GreyHole Attack, the node Burst Faults for a specific amount of time which is chosen randomly after running out of some specified time which will also be chosen randomly between 0 and MAX_TIME_TO_BURST_FAULT.

5. Results and Analysis

A network of fixed number of nodes has been constructed in the JiST SWANS simulator with the parameters given in the Table 4.1. Each of the nodes is initially made to follow standard AODV routing protocol in order to route the packets from source node to the destination. Later under the influence of attacks, malicious nodes follow a modified version of standard AODV in order to simulate the attacked environment. In all the scenarios, the Packet Throughput of the network has been considered to evaluate the effect of discussed attack models on AODV. Packet Throughput can be defined as the ratio of packets received by the destination to the number of packets sent (%). The behavior of this metric has been observed using standard AODV for each attack type under various proportions of malicious nodes. Later Simple Trusted AODV and the proposed Trusted Power Aware AODV have been used on the same network for improved performance of the network.

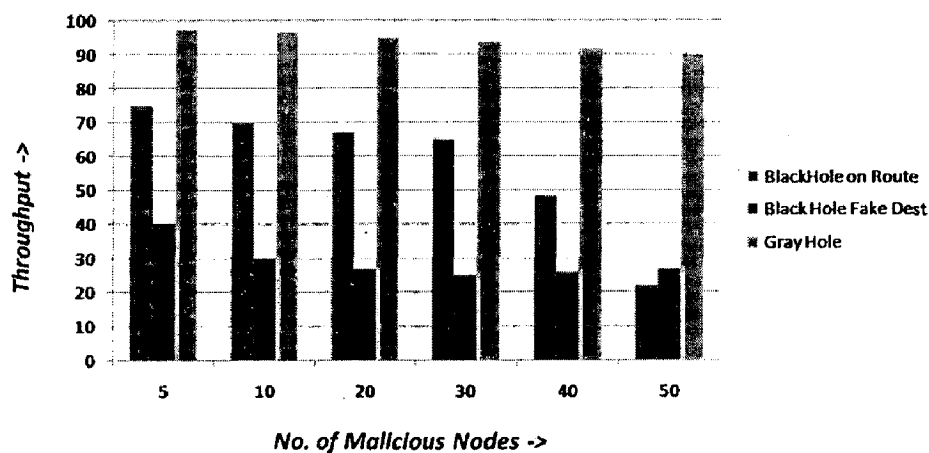


Figure 5.1: Throughput comparison with varying number of malicious nodes following specified attacks on AODV

All the results have been taken as the average of 20 simulation runs of the network in each of the case in order to quantify the throughput effectively.

As shown in Figure 5.1, as the number of malicious nodes is increased each attack type reduces throughput of the network in standard AODV, thereby hampering the performance of network drastically. A small number of blackhole nodes dramatically reduces throughput, the effect stabilizes for moderate numbers, and for Blackhole-OnRoute falls off for high numbers. Blackhole-FakeDest does not fall off further since throughput has already fallen significantly. The Greyhole attack results in a fairly gradual reduction in throughput as the number of malicious nodes increases. As predicted, Blackhole-FakeDest has the most effect over the network performance. For AODV, increasing the number of Blackhole-FakeDest nodes very soon reduces throughput while a similar number of Blackhole-OnRoute nodes gives better throughput. This clearly indicates the fact that the Blackhole-FakeDest is the one which affects the network the most as it fakes to has the Fresh Route to the Destination every time it receives the RREQ messages from its neighbors.

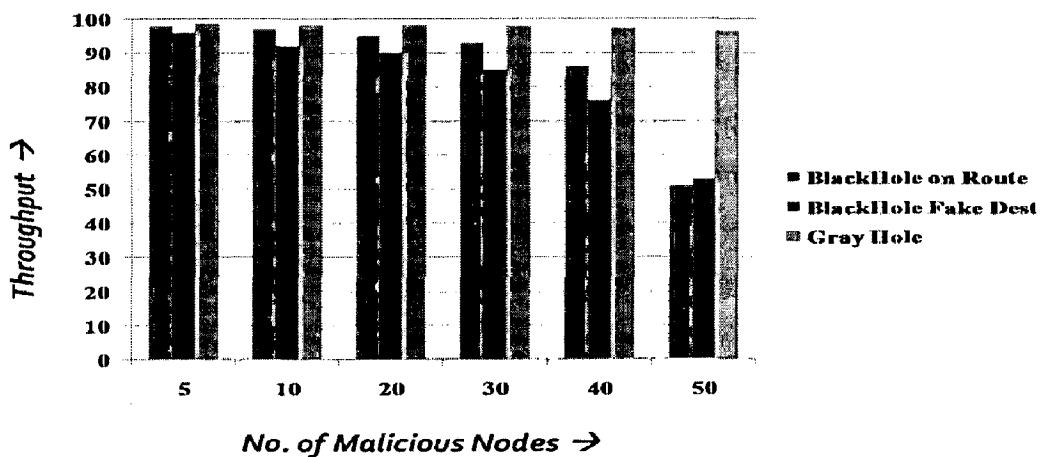


Figure 5.2: Throughput comparison with varying number of malicious nodes following specified attacks on Simple Trust Model without considering Battery Energy for Routing Decisions.

In Figure 5.2, the same network which has malicious nodes suffering from specified attacks has been executed over Simple Trusted AODV protocol wherein no battery life time has been considered for routing decisions. We can clearly observe that the number of packets delivered to the destination in this case is far improved when compared to the standard AODV protocol as shown in Figure 5.2. These throughput results are in accordance with the results obtained by Graffith et. al. [31] wherein authors propose a similar trust model against the network hampered with route misbehavior attacks.

Figure 5.3 shows the throughputs of same network with differing number of malicious nodes when the network is made to follow the proposed Secure Trusted Power Aware AODV protocol. As one can observe from the graph obtained in figure 5.3, there is a significant improvement in the percentage of throughput when compared to the previous trusted model which doesn't take any battery power into consideration. The improvement is as expected because while routing remaining battery power of the neighboring node also forms a major factor in routing decision along with the trust value for secured routing.

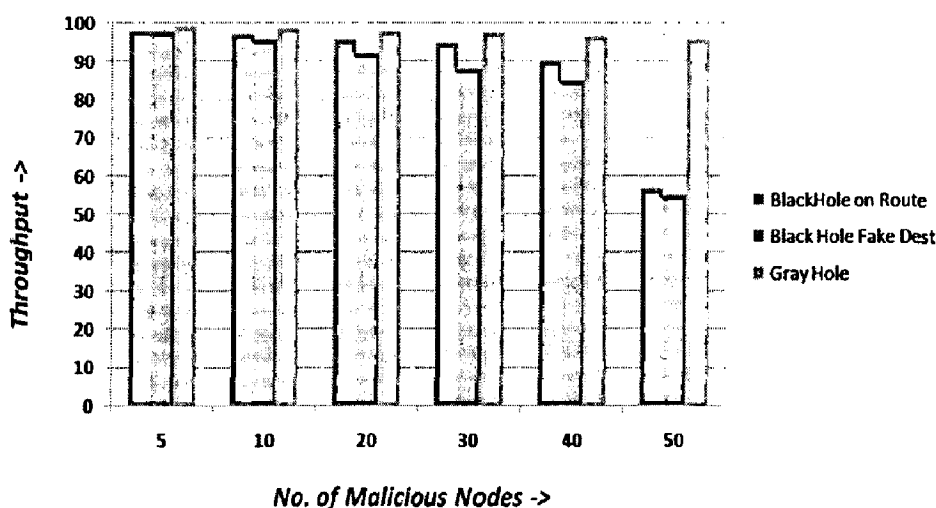


Figure 5.3: Throughput comparison with varying number of malicious nodes following specified attacks on Secure Trusted Power Aware AODV

In order to quantify the measure of improvement over the existing simple trust model without battery power consideration, we compare the two graphs obtained for specific scenarios. For example, for a network with 20 malicious Blackhole Fake Dest nodes, we can observe that our method improves the throughput of the network by a factor of 3 compared to the previous simple trust model. Thus, one can conclude from this explanation that the throughput of the network can be improvised effectively when both remaining battery energy of the node and trust in the node are considered while taking the routing decisions in the network. Apart from the improvement in the throughput, we can also conclude that the network is robust against various route misbehavior security threats present in the ad hoc network environment.

6. Conclusion and Future Work

6.1 Conclusion

Security and Energy Consumption are two such important features that they could determine the success and wide deployment of MANET. From the work that has been carried out in this dissertation work, we can draw the following conclusions.

- A variety of route misbehavior attacks have been identified and their models have been developed successfully by altering the standard code of AODV protocol.
- The impact of these developed attacks in the network reduces the overall throughput of the network as shown in the simulation study.
- A Power Aware Trust Mechanism has been developed which increases the throughput of the network considerably even in the presence of attacks.
- In order to quantify the work more lucidly consider a scenario for a specific case of 20 malicious Blackhole OnRoute nodes in a network of 50 nodes. The results obtained show that the throughput of the network has been improved from 93 to 96 compared to the previous simple non energy aware trust model.
- Using the proposed methodology of trust calculation, the effects of these attacks has been minimized and the network has been protected effectively against all three attacks.

Hence one can conclude from the results obtained, efficient detection techniques such as Trust based Detection Techniques need to be followed in order to identify the malicious nodes in the network and avoid considering them in taking routing decisions.

6.2 Future Directions

The research on MANET is still in an early stage. One of the key research challenges in routing algorithms is to exploit the knowledge about nodes' context in order to improve the overall performance of the network. Few of the key research issues related to the presented work in this dissertation and the future approach towards solving them can be summarized as follows.

- Existing proposals of securing the networks are typically based on one specific attack. They could work well in the presence of designated attacks, but there are many unanticipated or combined attacks that remain undiscovered.
- A lot of research is still on the way to identify new threats and create secure mechanisms to counter those threats with the rapid development in the field of communication networks.
- More research can be done on the robust key management system, trust-based protocols and energy aware routing, integrated approaches to routing security, and data security at different layers.
- More flexible sanctions against untrusted nodes, such as temporary blacklisting can also be investigate while building the trust model.
- Apart from the packet throughput, several other factors like source to destination delay, the packet overhead involved in the transmission etc., can also be

considered in evaluating the performance of the proposed secure power aware trust model in the network.

- The design of this trust model can be extended to handle special type of collaborative attacks like worm-hole attacks where the malicious nodes collaborate with each other to hamper the network.

These few above recommendations can be taken into account along with the ones given in the literature while proceeding with the future developments of the proposed methodology of trust establishment and thus the proposed model can be made more robust and flexible to suit the changing scenarios of variety of attacks in the field of mobile ad hoc networks.

REFERENCES

- [1] E. Royer and C. Toh, "A review of current routing protocols for ad hoc mobile wireless networks," in *Proc. Of Personal Communications, IEEE*, pp. 46–55, 1999.
- [2] J. Broch, D. Maltz, D. Johnson, Y. Hu, and J. Jetcheva "A performance comparison of multi-hop wireless ad hoc network routing protocols.", in *Proc. of the 4th annual ACM/IEEE international conference on Mobile computing and networking*, pp. 85–97, 1998.
- [3] Bing Wu, Jianrnin Chen, Jie Wu, Michaela Cardei, *A survey on Attacks and Countermeasures in Mobile Ad hoc Networks*, Florida Atlantic University, Wireless/Mobile Network Security, Chapter 12, Springer 2006.
- [4] M. Blaze, J. Feigenbaum, and J. Lacy, "Decentralized Trust Management," in *Proc. of the IEEE Symposium on Security and Privacy*, pp. 164 – 173, May 1996.
- [5] C. Ellis, "Leveraging IPv6 Capabilities to facilitate the deployment of Mobile Ad Hoc and Sensor Networking", in *2004 IPv6 Summit*, Dec. 2004.
- [6] IETF Internet Engineering Task Force, RFC2501, "MANET Routing Protocol Performance Issues and Evaluation Considerations," <http://www.ietf.org/rfc/rfc2501.txt>.
- [7] M. Fotino, A. Gozzi, J. Cano, C. Calafate, F. De Rango, P. Manzoni, S. Marano, "Evaluating Energy Consumption of Proactive and Reactive Routing Protocols in a MANET", in *IFIP International Federation for Information Processing*, vol. 248, Wireless Sensor and Adhoc Networks, pages 119-130, Springer, 2007.
- [8] Y. Hu and A. Perrig, "A Survey of Secure Wireless Ad Hoc Routing", in *IEEE Security & Privacy, special issue on Making Wireless Work*, vol. 2, no. 3, pp. 28-39, 2004.
- [9] B. Awerbuch, D. Holmer, C. Nita-Rotaru, and H. Rubens, "An On-demand Secure Routing Protocol Resilient to Byzantine Failures", *Proceedings of the ACM Workshop on Wireless Security*, pp. 21-30, 2002.
- [10] Y. Hu, A Perrig, and D. Johnson, "Packet Leashes: A Defense Against Wormhole Attacks in Wireless Ad Hoc Networks," in *Proceedings of IEEE INFORCOM*, 2002.
- [11] S. Singh, M. Woo, and C. S. Raghavendra. "Power-aware routing in mobile ad hoc networks", in *Proceedings of ACM MobiCom*, pp. 181–190, 1998.

- [12] D.H.McKnight and N.L.Chervany, "The Meanings of Trust. Technical Report MISRC Working Paper Series 96-04", University of Minnesota, Management Information Systems Research Center, 1996.
- [13] D. Gambetta, "Can We Trust Trust?" in D. Gambetta, editor, "*Trust: Making and Breaking Cooperative Relations*," Basil Blackwell. Oxford, pp. 213-238, 1990.
- [14] R. Falcone and C. Castelfranchi, "Social Trust: A Cognitive Approach," pp. 55-99. Kluwer, 2001.
- [15] D.H.McKnight and N.L.Chervany, "The Meanings of Trust," Technical Report MISRC Working Paper Series 96-04, University of Minnesota, Management Information Systems Research Center, 1996.
- [16] T. Grandison and M. Sloman. "A Survey of Trust in Internet Applications," *IEEE Communications Surveys and Tutorials*, 3, 2000.
- [17] D.W. Manchala, "Trust Metrics, Models and Protocols for Electronic Commerce Transactions," in *Proceedings of the 18th International Conference on Distributed Computing Systems*, Netherlands, May 1998.
- [18] A. Josang and S. Lo Presti. , "Analysing the Relationship Between Risk and Trust," In T. Dimitrakos, editor, in *Proc. of the Second International Conference on Trust Management (iTrust)*, Oxford, March 2004.
- [19] A. Josang and S. Pope, "Semantic Constraints for Trust Transitivity," in S. Hartmann and M. Stumptner, editors, in *Proceedings of the Asia-Pacific Conference of Conceptual Modelling (APCCM)*, Newcastle, Australia, Feb. 2005.
- [20] S. Tadelis, "Firm Reputation with Hidden Information," *Economic Theory*, Vol.21, no. 6 pp. 635-651, 2003.
- [21] P. Resnick, R. Zeckhauser, R. Friedman, and K. Kuwabara, "Reputation Systems," *Communications of the ACM*, pp. 45-48, Dec. 2000.
- [22] J. Li, R. Li, and J. Kato, "Future Trust Management Framework for Mobile Ad Hoc Networks: Security in Mobile Ad Hoc Networks," *IEEE Communications Magazine*, vol. 46, no. 4, pp. 108-114, Apr. 2008.
- [23] M. Blaze, J. Feigenbaum, and J. Lacy, "Decentralized Trust Management," in *Proc. of IEEE Symposium on Security and Privacy*, pp. 164 – 173, 6-8 May, 1996.

- [24] K. Paul and D. Westhoff, "Context-Aware Detection of Selfish Nodes in DSR based Ad Hoc Networks," in *Proc. of IEEE Globecom Conf.*, Taipei, Taiwan, 2002.
- [25] Jin-Hee Cho and Ananthram Swami, "Towards Trust-based Cognitive Networks: A Survey of Trust Management for Mobile Ad Hoc Networks", *U.S.Army Research Laboratory, in 14th ICCRTS*, 2008.
- [26] Y. L. Sun, W. Yu, Z. Han, and K. J. R. Liu, "Information Theoretic Framework of Trust Modeling and Evaluation for Ad Hoc Networks," *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 2, pp. 305-317, Feb. 2006.
- [27] J. Golbeck, "Computing with Trust: Definition, Properties, and Algorithms," in *proceedings of Securecomm and Workshops-Security and Privacy for Emerging Areas in Communications Networks*, Baltimore, MD, pp. 1-7, Aug.,2006.
- [28] T. Jiang and J. S. Baras, "Ant-based Adaptive Trust Evidence Distribution in MANET," *Proc. 2nd Int'l Conf. on Mobile Distributed Computing Systems Workshops (MDC)*, Tokyo, Japan, pp. 588-593, 23-24 March 2004.
- [29] Theodorakopoulos and J. S. Baras, "On Trust Models and Trust Evaluation Metrics for Ad Hoc Networks," *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 2, pp. 318-328, Feb. 2006.
- [30] Boukerche and Y. Ren, "A Security Management Scheme using a Novel Computational Reputation Model for Wireless and Mobile Ad Hoc Networks," *Proc. of Int'l Workshop on Modeling Analysis and Simulation of Wireless and Mobile Systems*, Vancouver, British Columbia, Canada, pp. 88-95, 2008.
- [31] Nathan Griffiths, Arshad Jhumka, Anthony Dawson and Richard Myers, "A Simple Trust model for On-Demand Routing in Mobile Ad-hoc Networks" , in *IDC-2008*, Department of Computer Science, University of Warwick, 2008.
- [32] Vinay Rishiwal, S. Verma and K. Bajpai.S.: " QoS Based Power Aware Routing in MANETs", *International Journal of Computer Theory and Engineering*, Vol. 1, No. 1, pp. 1793-8201,2009.
- [33] Ladislav Huraj and Helmut Reiser, "VO Intersection Trust in Ad Hoc Grid Environment", in *Proceedings of the 2009 Fifth International Conference on Networking and Services*, pp. 456-461, 2009.
- [34]"Promiscuous Mode," *Wikipedia*, at http://en.wikipedia.org/wiki/Promiscuous_mode.

- [35] S. McCanne and S. Floyd. “ns (Network Simulator),” <http://www-nrg.ee.lbl.gov/ns>, 1995.
- [36] G. Riley, R. M. Fujimoto, and M. A. Ammar, “A generic framework for parallelization of network simulations,” in *MASCOTS*, Mar. 1999.
- [37] G. Riley and M. Ammar, “Simulating large networks: How big is big enough?,” In *Conference on Grand Challenges for Modeling and Sim.*, Jan. 2002.
- [38] X. Zeng, R. L. Bagrodia, and M. Gerla. GloMoSim: a library for parallel simulation of large-scale wireless networks. In *PADS*, May 1998.

LIST OF PUBLICATIONS

1. Naga Sathish Gidijala, Sanketh Datla and R.C.Joshi, “**A Robust Trust Mechanism Algorithm for Secure Power Aware AODV Routing in Mobile Ad hoc Networks**”, Accepted for Publication in the *Proceedings of Third International Conference on Contemporary Computing IC3-2010*, (in Communications in Computer and Information Science ISSN: 1865-0929), Springer, 2010.
2. Naga Sathish Gidijala, Sanketh Datla and R.C.Joshi, “**A Robust Trust Mechanism for Secure Power Aware AODV Routing in Mobile Ad hoc Networks**”, in the *Proceedings of National Conference on Emerging Trends and Applications in Computer Science (ISBN : 978-80-910147-0-9)*, St.Anthony’s College, Shillong, pp. 167-171, April 2010.