

# Propagating Trust in Ad-hoc Networks for Reliable Routing

Asad Amir Pirzada, Amitava Datta and Chris McDonald  
School of Computer Science & Software Engineering  
The University of Western Australia

# Sequence of Presentation

- Routing Protocols
- Vulnerabilities
- Security Models
- Trust & Security Issues
- Proposed Trust Model
- Extension to DSR
- Analysis
- Conclusion

# Routing Protocols

## Reactive

- Dynamic Source Routing (DSR)
- Ad-hoc On-Demand Distance Vector (AODV)
- Temporally Ordered Routing Algorithm (TORA)

## Proactive

- Optimized Link State Routing Protocol (OLSR)
- Destination-Sequenced Distance Vector (DSDV)

# Vulnerabilities in Routing Protocols

- Lack of Trust Infrastructure
- Implicit Trust-your-Neighbour Relationships
- Presence of malicious and compromised nodes
- Route buildup by intermediate nodes

# Secure Routing Protocols

- Authenticated Routing for Ad-hoc Networks (**ARAN**) : 2002
- **ARIADNE** : 2002
- Secure Ad-hoc On-Demand Distance Vector (**SAODV**) : 2001
- Security-Aware Ad-hoc Routing (**SAR**) : 2001
- Secure Efficient Distance Vector (**SEAD**) : 2002
- Secure Link State Routing Protocol (**SLSP**) : 2002
- Secure Routing Protocol (**SRP**) : 2002

# Comparison

<b>Performance Parameters</b>	<b>ARAN</b>	<b>ARIADNE</b>	<b>SAODV</b>	<b>SAR</b>	<b>SEAD</b>	<b>SLSP</b>	<b>SRP</b>
<b>Type</b>	Reactive	Reactive	Reactive	Reactive	Proactive	Proactive	Reactive
<b>Encryption Algorithm</b>	Asymmetric	Symmetric	Asymmetric	Symmetric/ Asymmetric	Symmetric	Asymmetric	Symmetric
<b>MANET Protocol</b>	AODV /DSR	DSR	AODV	AODV	DSDV	ZHLS	DSR/ZRP
<b>Synchronization</b>	No	Yes	No	No	Yes	No	No
<b>Central Trust Authority</b>	CA Required	KDC Required	CA Required	CA/KDC Required	CA Required	CA/KDC Required	CA Required
<b>Authentication</b>	Yes	Yes	Yes	Yes	Yes	Yes	Yes
<b>Confidentiality</b>	Yes	No	No	Yes	No	No	No
<b>Integrity</b>	Yes	Yes	Yes	Yes	No	No	Yes
<b>Non-repudiation</b>	Yes	No	Yes	Yes	No	Yes	No
<b>Anti - Spoofing</b>	Yes	Yes	Yes	Yes	No	Yes	Yes
<b>DoS Attacks</b>	No	Yes	No	No	Yes	Yes	Yes

# Types of Ad-hoc Networks

- Managed
  - Limited size
  - Trusted Third Party
  - Pre-Configuration
- Pure
  - No size limitation
  - No assumptions
  - Resembles the Human Trust Model

# What is Security ?

- Trust in the Trusted Third Party
- Trust in the Cryptographic Mechanism
- Trust in the Key

“No amount of general beta testing will reveal a security flaw and there is no test possible that can prove the absence of flaws” *Bruce Schneier*

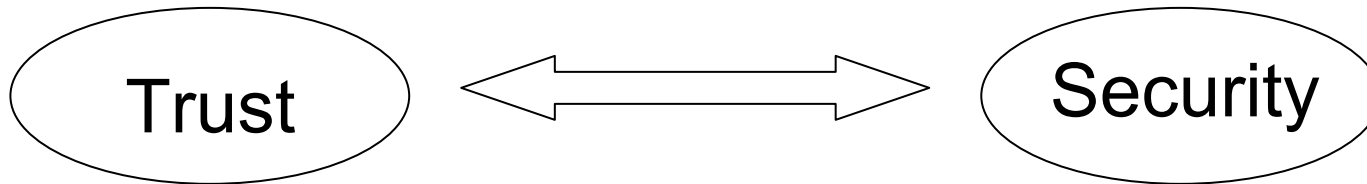


# Trust & Security

“Security makes trust work”

or does

“Trust makes security work” ?



- Realistic
- Uni-directional
- Non-transitive
- Not absolute
- Dynamic

- Idealistic
- Bi-directional
- Transitive
- Absolute
- Static

# Trust

- Mayer, Davis and Schoorman (1995)

The **willingness of a party to be vulnerable** to the actions of another party based on the expectation that the other party will perform a particular action important to the trustor, irrespective of the ability to monitor or control the party.

- Jøsang (1996)

Trust in a passionate entity (human) is the **belief** that it will behave without malicious intent and trust in a rational entity (system) is the **belief** that it will resist malicious manipulation. (honest & straight)

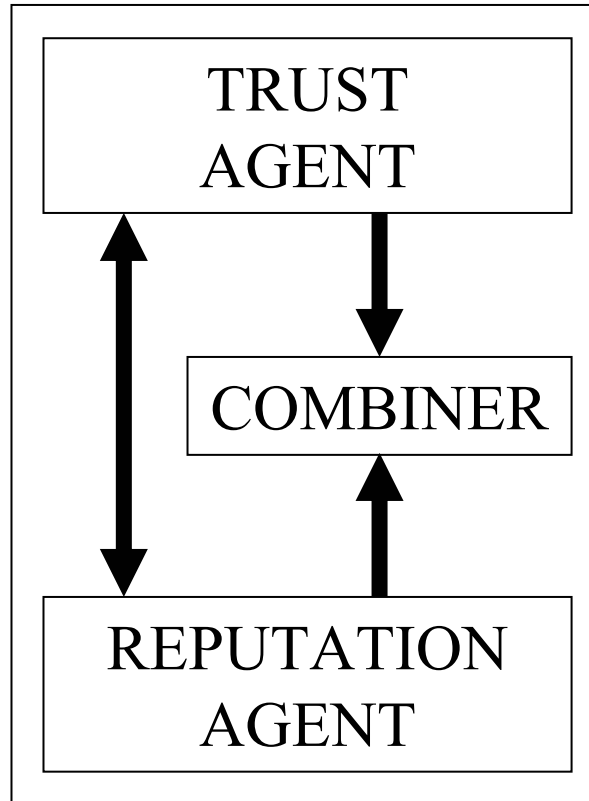
- Denning (1993)

Trust cannot be treated as a property of trusted systems but rather it is an **assessment based on experience** that is shared through networks of people

# Types of Trust

- Direct
  - Experience based
  - Reliability
- Indirect
  - Reference
  - Credibility

# Trust Model



# Trust Agent

- Trust Derivation
- Trust Quantification
- Trust Computation

<b>OSI</b>	<b>PROPOSED</b>	<b>TCP/IP</b>
Application	Computation & Quantification	Application
Presentation		
Session		
Transport	Derivation	Transport
Network		Internet
Data link		Host to Network
Physical		

# Trust Agent

....contd

## Trust Derivation

- Passive learning
  - Promiscuous mode
  - Forwarding
- Filtering

# Trust Agent

....contd

## Trust Quantification

- Normalization of Trust Categories

$$C_i = \frac{C_s - C_f}{C_s + C_f} \quad \text{for } C_s + C_f \neq 0 \quad \text{else } C_i = 0$$

<b>Value</b>	<b>Representation</b>
-1	Absolute Distrust
$-1 < \text{Trust} < 0$	Distrusting
0	Ignorance
$0 < \text{Trust} < +1$	Trusting
+1	Absolute Trust

# Trust Agent

....contd

## Trust Computation

- Dynamic assignment of situational weights
- Varies with type of application and time

Unimportant  $0 \leq \text{Weight} \leq 1$  Most important

Trust in node  $y$  by node  $x$

$$T_{xy} = \sum_{i=1}^n [ W(i) \times T_{xy}(i) ]$$

where  $W(i)$  is the weight of the  $i^{th}$  trust category to  $x$  and  $T_{xy}(i)$  is the situational trust of  $x$  in the  $i^{th}$  trust category of  $y$ .

# Reputation Agent

## HashCash

- CPU Cost Factor
- Effort based disincentive

<b>VERSION</b>	<b>TIME</b>	<b>RESOURCE</b>	<b>TRIAL</b>
----------------	-------------	-----------------	--------------

Cryptographic Hash



HashCash Token

# Reputation Agent

....contd

## 1. Requester → Recommender ( Rec\_Req )

$ID_{RQ}$ ,  $ID_{RRQ}$ ,  $ID_{TT}$ , Hash {Ver, TS,  $ID_{REC}$ , Trial}

## 2. Recommender → Requester ( Rec\_Rep )

$ID_{RRQ}$ ,  $T_T$

$ID_{RQ}$  Identity of Requesting Node

$ID_{REC}$  Identity of Recommending Node

$ID_{TGT}$  Identity of Target Node

$ID_{RRQ}$  Unique Rec\_Req number

$ID_{TT}$  Identity of Trust Type

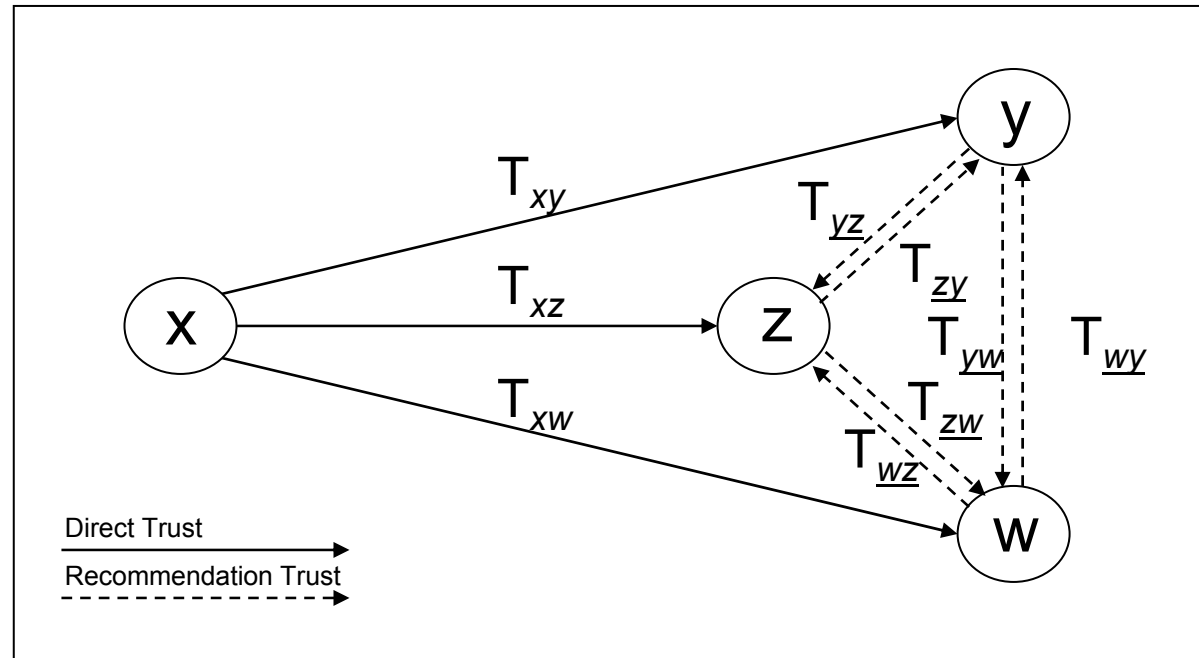
$T_T$  Value of Trust Type

Ver Identity of hash function

TS Informs of date and time when this message was generated

Trial Number to be determined in order to generate a valid token

# Combiner



$$T_{xzy} = T_{xz} \odot T_{zy} = 1 - (1 - T_{xz})^{T_{zy}}$$

$$T(y) = 1 - (1 - T_{xy}) \cdot (1 - T_{xzy}) \cdot (1 - T_{xwy})$$

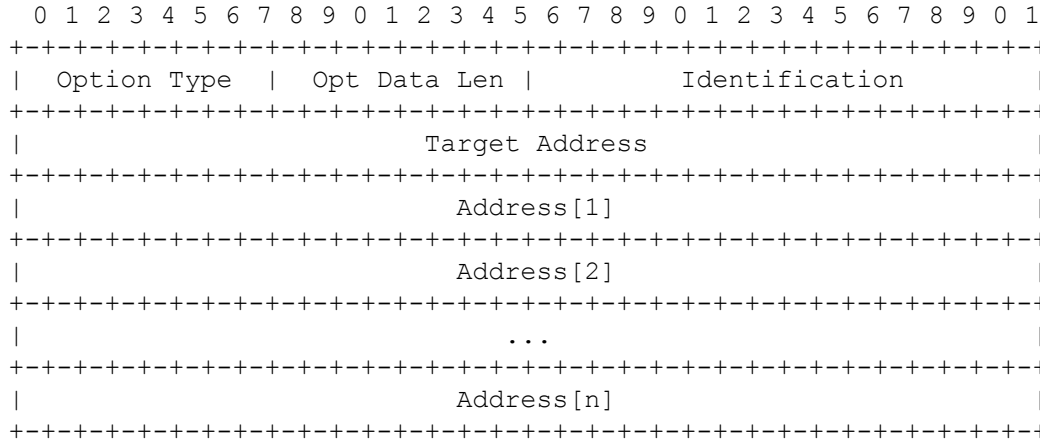
# Extension to Dynamic Source Routing (DSR) Protocol

# DSR : Salient Features

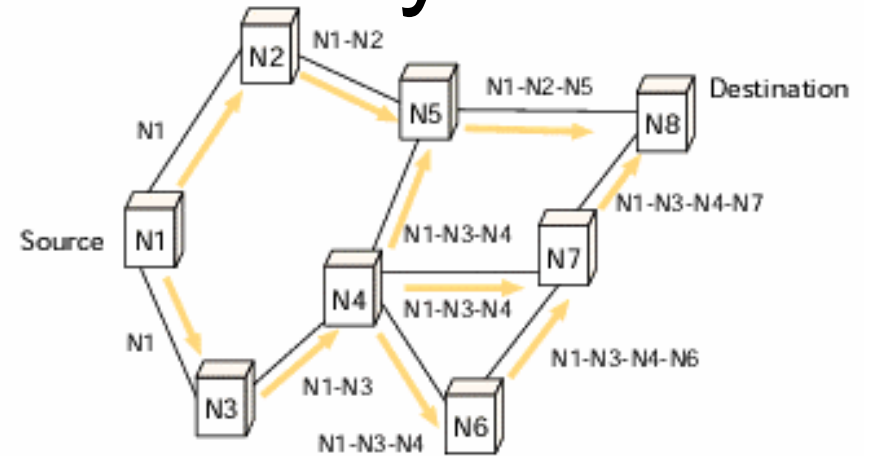
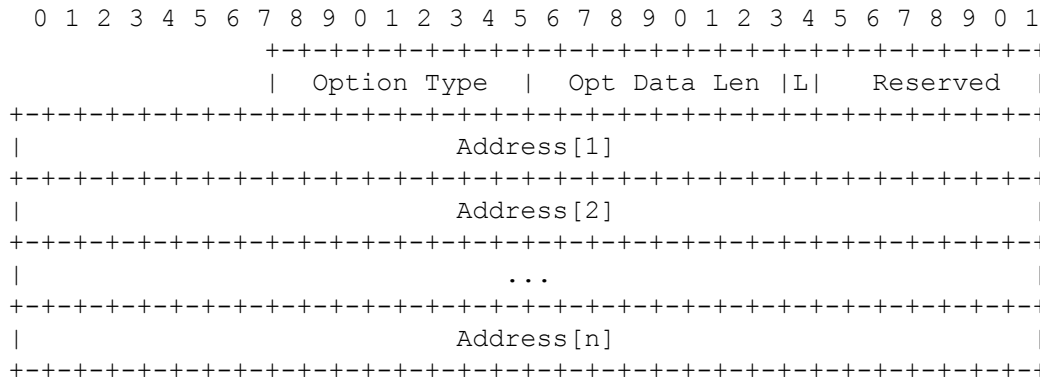
- Source routing
  - Complete path contained in each packet
- Route discovery
  - Flooding of route request till a node replies
- Route maintenance
  - Explicit link breakage notification
- Route Caching
  - Path Cache
  - Link Cache

# DSR : Route Discovery

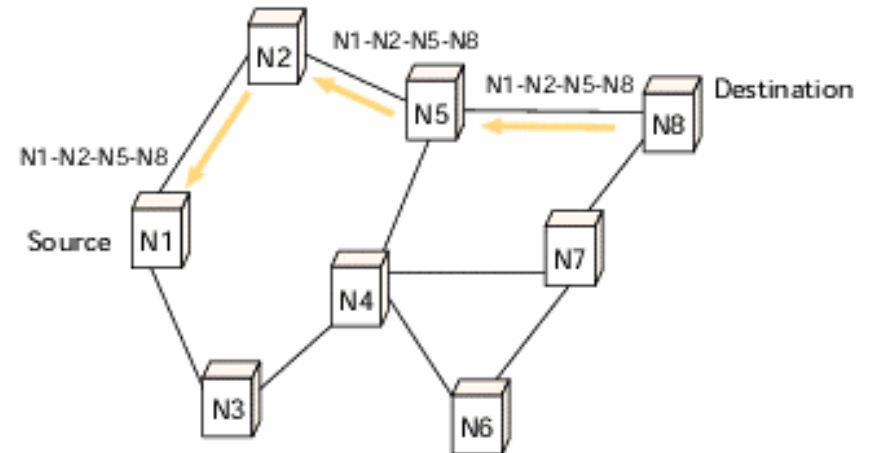
## ROUTE REQUEST (RREQ) MESSAGE FORMAT



## ROUTE REPLY (RREP) MESSAGE FORMAT



(a) Building of the route record during route discovery



(b) Propagation of the route reply with the route record

# Quantification of Trust Categories

- Acknowledgements ( $P_A$ )
- Packet Precision ( $P_P$ )
- Gratuitous Route Replies ( $G_R$ )
- Blacklists ( $B_L$ )
- Salvaging ( $S_G$ )

# Application of the Trust Agent

$$T_{xy} = W(P_A) \times T_{xy}(P_A) + W(P_P) \times T_{xy}(P_P) + W(G_R) \times T_{xy}(G_R) + W(B_L) \times T_{xy}(B_L) + W(S_G) \times T_{xy}(S_G)$$

Node	Situational Trust					Direct Trust
	Passive Ack	Packet Prec	Grat Route Replies	Black Lists	Salvage Route Replies	
w	$T_{xw}(P_A)$	$T_{xw}(P_P)$	$T_{xw}(G_R)$	$T_{xw}(B_L)$	$T_{xw}(S_G)$	$T_{xw}$
y	$T_{xy}(P_A)$	$T_{xy}(P_P)$	$T_{xy}(G_R)$	$T_{xy}(B_L)$	$T_{xy}(S_G)$	$T_{xy}$
z	$T_{xz}(P_A)$	$T_{xz}(P_P)$	$T_{xz}(G_R)$	$T_{xz}(B_L)$	$T_{xz}(S_G)$	$T_{xz}$
...	...	...	...	...	...	...
...	...	...	...	...	...	...

DSR Situational and Direct Trust Table

# Application of the Reputation Agent

Node	w	y	z	...	...
w		$T_{wy}$ $T_{wy}(P_A)$ $T_{wy}(P_P)$ $T_{wy}(G_R)$ $T_{wy}(B_L)$ $T_{wy}(S_G)$	$T_{wz}$ $T_{wz}(P_A)$ $T_{wz}(P_P)$ $T_{wz}(G_R)$ $T_{wz}(B_L)$ $T_{wz}(S_G)$	...	...
y	$T_{yw}$ $T_{yw}(P_A)$ $T_{yw}(P_P)$ $T_{yw}(G_R)$ $T_{yw}(B_L)$ $T_{yw}(S_G)$		$T_{yz}$ $T_{yz}(P_A)$ $T_{yz}(P_P)$ $T_{yz}(G_R)$ $T_{yz}(B_L)$ $T_{yz}(S_G)$	...	...
z	$T_{zw}$ $T_{zw}(P_A)$ $T_{zw}(P_P)$ $T_{zw}(G_R)$ $T_{zw}(B_L)$ $T_{zw}(S_G)$	$T_{zy}$ $T_{zy}(P_A)$ $T_{zy}(P_P)$ $T_{zy}(G_R)$ $T_{zy}(B_L)$ $T_{zy}(S_G)$		...	...
...	...	...	...	...	...

DSR Reputation Table

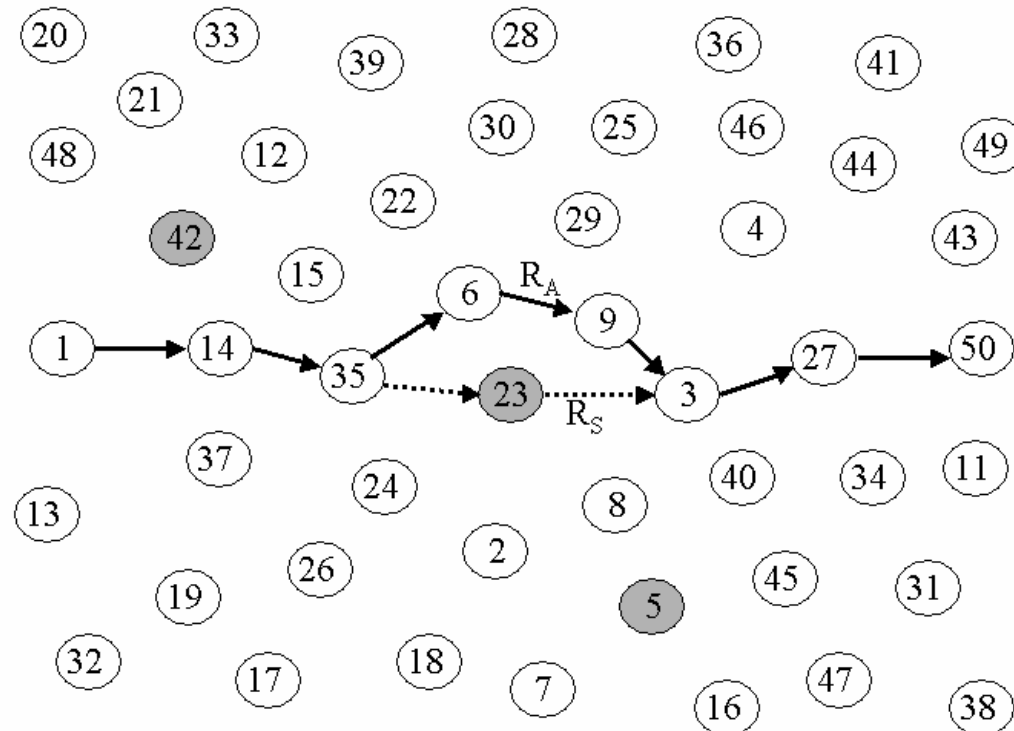
# Application of the Combiner

Node	Derived Trust via Node				Aggregate Trust
	w	y	z	...	
w		$T_{xyw}$	$T_{xzw}$	...	$T(w)$
		$1 - (1 - T_{xy})^{T_{yw}}$	$1 - (1 - T_{xz})^{T_{zw}}$	...	$1 - (1 - T_{xw}). (1 - T_{xyw}). (1 - T_{xzw})$
y	$T_{xwy}$		$T_{xzy}$	...	$T(y)$
	$1 - (1 - T_{xw})^{T_{wy}}$		$1 - (1 - T_{xz})^{T_{zy}}$	...	$1 - (1 - T_{xy}). (1 - T_{xzy}). (1 - T_{xwy})$
z	$T_{xwz}$	$T_{xyz}$		...	$T(z)$
	$1 - (1 - T_{xw})^{T_{wz}}$	$1 - (1 - T_{xy})^{T_{yz}}$		...	$1 - (1 - T_{xz}). (1 - T_{xyz}). (1 - T_{xwz})$
...	...	...	...	...	...

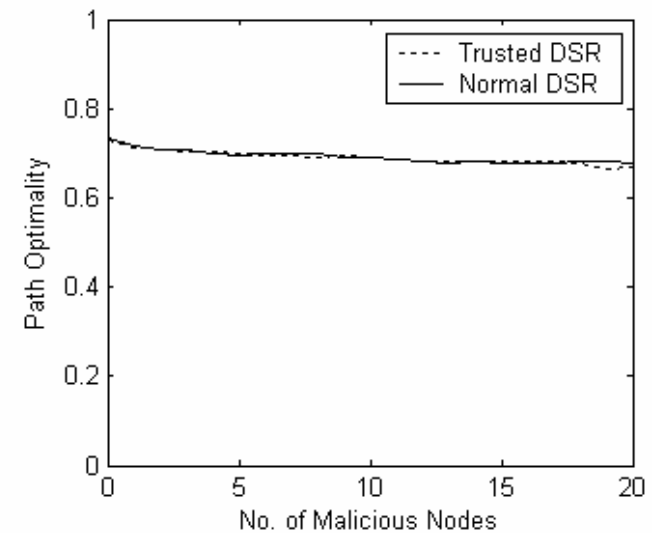
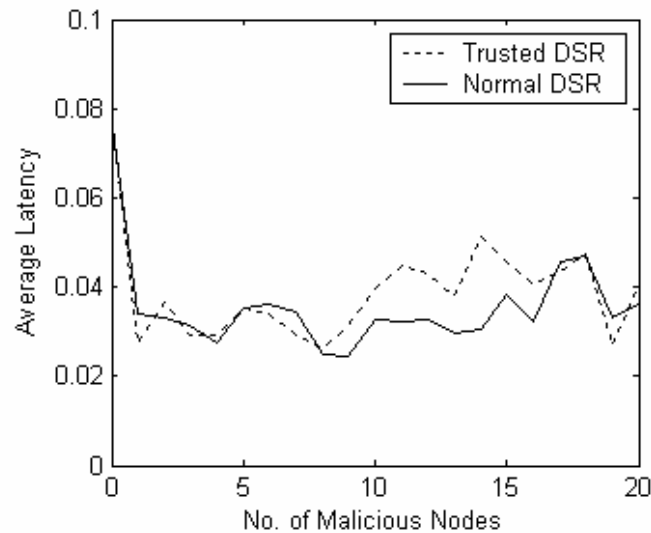
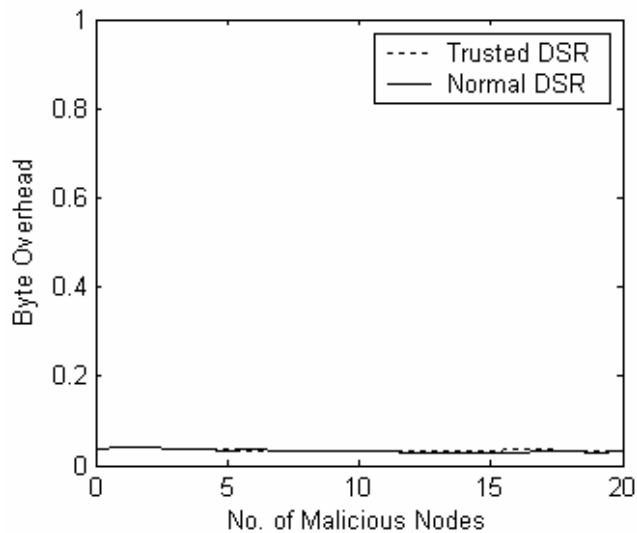
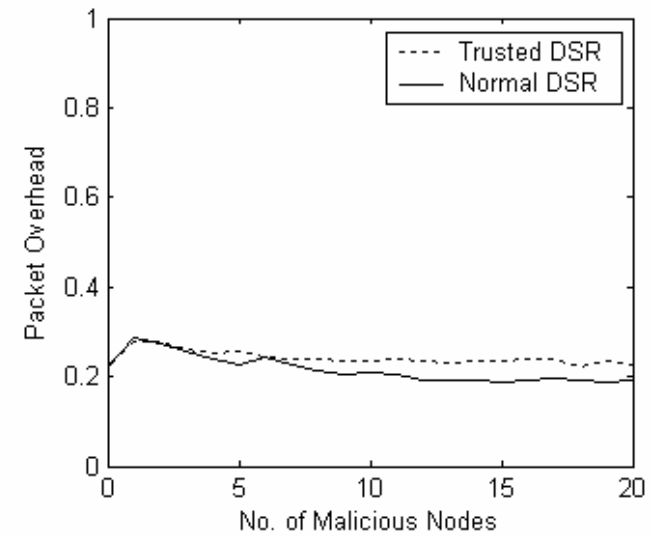
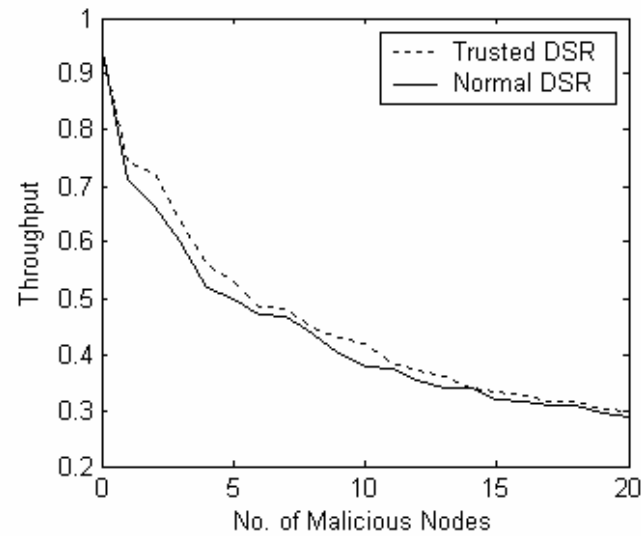
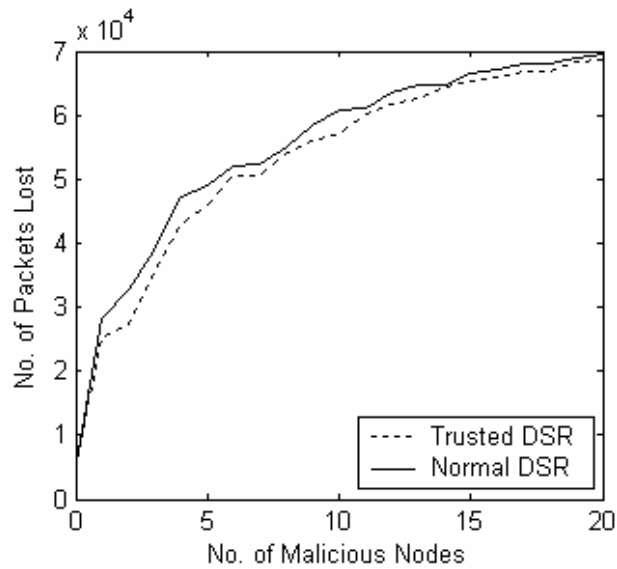
DSR Derived and Aggregate Trust Table

# Trustworthy Routing

- Association of aggregate trust levels to link cost
- Route selection based upon minimum hop count and maximum trust levels



# Initial Results



# Analysis

- HashCash Latency
- Fallacious Trust Build-up
- Differentiation of malevolent and benevolent behaviour
- Ambiguous/Receiver Collision Problems

# Conclusions

- Effort/Return Model
- Confidence measures
- Passive/Active mode of operation
- No requirement of Trusted Third Party
- Suitable for improvised on-the-fly networks

# Questions