A

Project Report

on

MANET FOR COMMUNICATION

Submitted in Partial Fulfillment of
the Requirements for the Degree
of

Bachelor of Engineering

in

Computer Engineering

to

Kavayitri Bahinabai Chaudhari
North Maharashtra University, Jalgaon

Submitted by

Girish Kumar Patnaik
Assad Saasd
Zxczxc Zxczxc Zxczxc
Qweqwe Eqweqw

Under the Guidance of

Prof. Dr. Girish K. Patnaik

DEPARTMENT OF COMPUTER ENGINEERING
SSBT's COLLEGE OF ENGINEERING AND TECHNOLOGY,
BAMBHORI, JALGAON - 425 001 (MS)
2018 - 2019

SSBT's COLLEGE OF ENGINEERING AND TECHNOLOGY, BAMBHORI, JALGAON - 425 001 (MS)

DEPARTMENT OF COMPUTER ENGINEERING

CERTIFICATE

This is to certify that the project entitled *MANET for Communication*, submitted by

Girish Kumar Patnaik
Assad Saasd
Zxczxc Zxczxc Zxczxc
Qweqwe Eqweqw

in partial fulfillment of the degree of *Bachelor of Engineering* in *Computer Engineering* has been satisfactorily carried out under my guidance as per the requirement of Kavayitri Bahinabai Chaudhari North Maharashtra University, Jalgaon.

Date: September 25, 2018
Place: Jalgaon

Prof. Dr. Girish K. Patnaik
Guide

Prof. Dr. Girish K. Patnaik
Head

Prof. Dr. K. S. Wani
Principal

Acknowledgements

Hello how are you? vvvvvvvvvv vvvvvvvvvvvvvv vvvvvvvvvv vvvvvvvvvvv vvvvvvv vvvvvvvvv vvvvvvvvvvvvvvvvv

Girish Kumar Patnaik
Assad Saasd
Zxczxc Zxczxc Zxczxc
Qweqwe Eqweqw

Abbreviations

AIMD Additive Increment and Multiplicative Decrement

MANET Mobile Ad-hoc Network

Contents

List of Tables

List of Figures

Abstract

However, MANETs offer a convenient infrastructure-less communication over a shared wireless channel. These, being cost-effective and quick to install, find many applications such as military tactical operations, emergencies and law enforcement, rescue missions, and many other applications like round table conferences and classroom discussions etc. In brief, MANET characteristics are as enumerated below.

However, MANETs offer a convenient infrastructure-less communication over a shared wireless channel. These, being cost-effective and quick to install, find many applications such as military tactical operations, emergencies and law enforcement, rescue missions, and many other applications like round table conferences and classroom discussions etc. In brief, MANET characteristics are as enumerated below.

Chapter 1

Introduction

The wireless communication technologies have evolved quickly over the past few years. The advances in wireless communication have enabled rapid development of a variety of wireless networks, such as wireless local area network, multi-hop ad-hoc network, and sensor network. In all these networks, a set of computing devices are interconnected over wireless medium to form a distributed environment. Popularity of these networks is due to its ubiquity and convenience.

Wired network with static hosts and routers form a fixed infrastructure for data communication. Replacement of these static hosts with wireless supported portable devices provide infrastructure supported wireless local area network. In such networks the routers are part of infrastructure and portable devices are mobile. Further, the wireless portable devices with built-in router provide multi-hop ad-hoc networks. Mobile Ad-hoc Networks (MANETs) are multi-hop ad-hoc networks where some or all of the devices may be mobile.

1.1 Mobile Ad-hoc Network

Mobile Ad-hoc Network (MANET) is a collection of autonomous nodes that form a dynamic purpose-specific multi hop radio network in a decentralized fashion [1] [2] [3]. As nodes move about in an unpredictable fashion, these networks must be configured on the fly to handle the dynamic topology. These networks with no fixed topology have been constrained with limited energy and processing capabilities of nodes and lack centralized administration. These networks also carry all the disadvantages of wireless medium like shared physical medium, higher bit error rates etc. However, MANETs offer a convenient infrastructure-less communication over a shared wireless channel. These, being cost-effective and quick to install, find many applications such as military tactical operations, emergencies and law enforcement, rescue missions, and many other applications like round table conferences and classroom discussions etc. In brief, MANET characteristics are as enumerated below.

1. There is no fixed topology.
2. Each node is a router.
3. The transmission medium is shared.

- There is no fixed topology.
- Each node is a router.
- The transmission medium is shared.

Mobile Ad-hoc Network (MANET) is a collection of autonomous nodes that form a dynamic purpose-specific multi hop radio network in a decentralized fashion [1] [2] [3]. As nodes move about in an unpredictable fashion, these networks must be configured on the fly to handle the dynamic topology. These networks with no fixed topology have been constrained with limited energy and processing capabilities of nodes and lack centralized administration. These networks also carry all the disadvantages of wireless medium like shared physical medium, higher bit error rates etc. However, MANETs offer a convenient infrastructureless communication over a shared wireless channel. These, being cost-effective and quick to install, find many applications such as military tactical operations, emergencies and law enforcement, rescue missions, and many other applications like round table conferences and classroom discussions etc. In brief, MANET characteristics are as enumerated below.

Mobile Ad-hoc Network (MANET) is a collection of autonomous nodes that form a dynamic purpose-specific multi hop radio network in a decentralized fashion [1] [2] [3]. As nodes move about in an unpredictable fashion, these networks must be configured on the fly to handle the dynamic topology. These networks with no fixed topology have been constrained with limited energy and processing capabilities of nodes and lack centralized administration. These networks also carry all the disadvantages of wireless medium like shared physical medium, higher bit error rates etc. However, MANETs offer a convenient infrastructureless communication over a shared wireless channel. These, being cost-effective and quick to install, find many applications such as military tactical operations, emergencies and law enforcement, rescue missions, and many other applications like round table conferences and classroom discussions etc. In brief, MANET characteristics are as enumerated below.

Mobile Ad-hoc Network (MANET) is a collection of autonomous nodes that form a dynamic purpose-specific multi hop radio network in a decentralized fashion [1] [2] [3]. As nodes move about in an unpredictable fashion, these networks must be configured on the fly to handle the dynamic topology. These networks with no fixed topology have been constrained with limited energy and processing capabilities of nodes and lack centralized administration.

These networks also carry all the disadvantages of wireless medium like shared physical medium, higher bit error rates etc. However, MANETs offer a convenient infrastructure-less communication over a shared wireless channel. These, being cost-effective and quick to install, find many applications such as military tactical operations, emergencies and law enforcement, rescue missions, and many other applications like round table conferences and classroom discussions etc. In brief, MANET characteristics are as enumerated below.

Mobile Ad-hoc Network (MANET) is a collection of autonomous nodes that form a dynamic purpose-specific multi hop radio network in a decentralized fashion [1] [2] [3]. As nodes move about in an unpredictable fashion, these networks must be configured on the fly to handle the dynamic topology. These networks with no fixed topology have been constrained with limited energy and processing capabilities of nodes and lack centralized administration. These networks also carry all the disadvantages of wireless medium like shared physical medium, higher bit error rates etc. However, MANETs offer a convenient infrastructure-less communication over a shared wireless channel. These, being cost-effective and quick to install, find many applications such as military tactical operations, emergencies and law enforcement, rescue missions, and many other applications like round table conferences and classroom discussions etc. In brief, MANET characteristics are as enumerated below.

Mobile Ad-hoc Network (MANET) is a collection of autonomous nodes that form a dynamic purpose-specific multi hop radio network in a decentralized fashion [1] [2] [3]. As nodes move about in an unpredictable fashion, these networks must be configured on the fly to handle the dynamic topology. These networks with no fixed topology have been constrained with limited energy and processing capabilities of nodes and lack centralized administration. These networks also carry all the disadvantages of wireless medium like shared physical medium, higher bit error rates etc. However, MANETs offer a convenient infrastructure-less communication over a shared wireless channel. These, being cost-effective and quick to install, find many applications such as military tactical operations, emergencies and law enforcement, rescue missions, and many other applications like round table conferences and classroom discussions etc. In brief, MANET characteristics are as enumerated below.

Mobile Ad-hoc Network (MANET) is a collection of autonomous nodes that form a dynamic purpose-specific multi hop radio network in a decentralized fashion [1] [2] [3]. As nodes move about in an unpredictable fashion, these networks must be configured on the fly to handle the dynamic topology. These networks with no fixed topology have been constrained with limited energy and processing capabilities of nodes and lack centralized administration. These networks also carry all the disadvantages of wireless medium like shared physical medium, higher bit error rates etc. However, MANETs offer a convenient infrastructure-less communication over a shared wireless channel. These, being cost-effective and quick

to install, find many applications such as military tactical operations, emergencies and law enforcement, rescue missions, and many other applications like round table conferences and classroom discussions etc. In brief, MANET characteristics are as enumerated below.

Mobile Ad-hoc Network (MANET) is a collection of autonomous nodes that form a dynamic purpose-specific multi hop radio network in a decentralized fashion [1] [2] [3]. As nodes move about in an unpredictable fashion, these networks must be configured on the fly to handle the dynamic topology. These networks with no fixed topology have been constrained with limited energy and processing capabilities of nodes and lack centralized administration. These networks also carry all the disadvantages of wireless medium like shared physical medium, higher bit error rates etc. However, MANETs offer a convenient infrastructure-less communication over a shared wireless channel. These, being cost-effective and quick to install, find many applications such as military tactical operations, emergencies and law enforcement, rescue missions, and many other applications like round table conferences and classroom discussions etc. In brief, MANET characteristics are as enumerated below.

Mobile Ad-hoc Network (MANET) is a collection of autonomous nodes that form a dynamic purpose-specific multi hop radio network in a decentralized fashion [1] [2] [3]. As nodes move about in an unpredictable fashion, these networks must be configured on the fly to handle the dynamic topology. These networks with no fixed topology have been constrained with limited energy and processing capabilities of nodes and lack centralized administration. These networks also carry all the disadvantages of wireless medium like shared physical medium, higher bit error rates etc. However, MANETs offer a convenient infrastructure-less communication over a shared wireless channel. These, being cost-effective and quick to install, find many applications such as military tactical operations, emergencies and law enforcement, rescue missions, and many other applications like round table conferences and classroom discussions etc. In brief, MANET characteristics are as enumerated below.

1.2 Summary

In this chapter, an overview of the problem statement along with its solution for the work contained in this dissertation is provided. In the next chapter, related work in the area of communication architecture for disaster rescue operations is presented.

Chapter 2

LaTex Basic Blocks

In MANET, each node works not only for itself but also for other nodes. Under hostile environments, such as post-disaster rescue operation scenarios, some nodes may misbehave for individual interest. The misbehavior, such as dropping and forging of packets, by nodes may paralyze the network. So, reputation or direct trust and recommendation are instrumental to deal with such misbehaving nodes in MANET. This chapter presents a trust management scheme to derive trustworthiness of nodes and path. It also presents a trust based routing protocol that incorporates the trust management scheme to discover trustworthy path in the MANET.

This chapter is organized as follows. Section 2.1 presents trust management scheme. The proposed trust based routing protocol is presented in section 2.2. Finally, summary of the chapter is given in the last section.

2.1 Trust Management Scheme

Trust computation is based not only on reputation but also on recommendation and context. Reputation is from direct observations and it's rating reflects the behavior of a node. Monitor is the data source for reputation. The monitor has the mechanism to observe the behavior of its one-hop neighbors and deliver current experience as either negative or positive in the range [-1, 1]. Based on the current observation/experience about a node, its reputation rating gets updated. Recommendation is the communicated reputation of a node by another node. The recommendation by the neighboring nodes contribute towards trustworthiness of a node. Subsequently, trustworthiness of the discovered path is the accumulation of trustworthiness of nodes on the discovered path, i.e., based on reputation, recommendation and context, a node calculates trustworthiness of the discovered path. In the proposed scheme the destination node is considered as the context.

Table 2.1: Cross-correlation of Monitored RERR and RREQ Events

Event		Monitored Node		
		Source Node	Intermediate Node (not under local repair)	
RERR	Recv.	True	True	True
RERR	Send		True	False
RREQ	Send	True		
RREQ	Recv.			
RREQ	Forward			
Reputation		+1	+1	$\times \frac{1}{2}$

2.1.1 Reputation Rating Update Function

we propose a reputation rating update function as shown in equation (2.1).

$$R_{i+1} = \begin{cases} min\left\{1, d * R_i + (1-d) * e_v\right\}, & \text{for } 0 \leq e_v \leq 1 \\ max\left\{-1, R_i + \frac{1}{2} * e_v * (R_i + 1)\right\}, & \text{for } -1 \leq e_v < 0 \end{cases} \tag{2.1}$$

$$\begin{aligned} Where \quad & \mathrm{R}_i : \text{Reputation at the instance } i \\ & \mathrm{e}_v\text{: Current Experience} \\ & \text{d: A constant between 0 and 1} \end{aligned}$$

where the interval for R_i and e_v is [-1, 1]. It employs additive increment and multiplicative decrement based on the current experience e_v. The function maps reputation rating from the interval [-1, 1] to a result in the interval [-1, 1]. In MANET, all nodes are cooperative by nature. Hence, initially it is expected that all nodes behave normally. So, an initial reputation of a node on any other node is 50%, i.e., ZERO in the interval [-1, 1]. For a fully positive experience with $\mathrm{e}_v = 1$, comparison with maximal trust value 1 is:

$$1 - R_{i+1} = d * (1 - R_i)$$

i.e., the distance of the trust value to the maximal trust value is decreased by a fraction of old distance. Similarly, for a fully negative experience with e_v = -1, comparison with maximal distrust value -1 is:

$$1 + R_{i+1} = \frac{R_i + 1}{2}$$

i.e., the distance of the trust value to the maximal distrust value is halved.

2.1.2 Trustworthiness of Node and Path

Let *R_i(x,y)* be the reputation rating of node y by node x at an instance *i*, then the recommendation, i.e., the communicated reputation rating, of the node y by node x is the same.

Table 2.2: Node Trust Table

Node Id	Node Trust Value

Table 2.3: Path Trust Table

Dest. Node Id	Trust Value

Accumulation of such recommendations by a node z at an instance i is:

$$R_i^z(x,y) = \bigcup\{R_i(x,y) \quad | \text{ for all x that are neighbor of z}\} \tag{2.2}$$

So, $R_i^y(x,y)$ is the accumulation of recommendations of the node y from all its neighbors x by the node y itself at the instance i. These recommendations by the neighboring nodes contribute towards trustworthiness of a node y, $T_i(y)$.

$$T_i(y) = f(R_i^y(x,y)) \tag{2.3}$$

where the function f can be *mean*, *median*, *mode*, *min* etc. Under hostile environments, *median* is the most suitable function as it thwarts outliers. Further, the trustworthiness of a node is computed for a given context, where context is the destination node. Recommendations pertaining to a specific destination node contribute towards trustworthiness of a node.

Trustworthiness of a discovered path from node x to destination node d is:

$$T_i(x,d) = \sum_y(T_i(y) \quad | \text{ for all } y \text{ from } x \text{ to } d \text{ in the discovered path}) \tag{2.4}$$

i.e., summation of trustworthiness of nodes along the discovered path.

Since by monitoring promiscuously the neighboring nodes along the discovered path have more conclusive information about the nodes on the discovered path, hence, recommendations by these neighboring nodes are employed to compute trustworthiness of the discovered path.

2.1.3 Data structure for Trustworthiness of Node and Path

Every node maintains node trust table, path trust table and trust reply table as shown in table 2.2, 2.3 and 2.4, respectively. Based on the current experience from the monitor, trust value of a node in the node trust table is updated as per the equation (2.1). Trust reply table is the accumulation of recommendations, as in equation (2.2). Trust replies are in the form of (recommender's node Id, recommended node trust value). The path trust table stores the trustworthiness of the path from current node to a destination as per the equation (2.4).

Further, in order to deal with malicious nodes, every node maintains alarm node trust table, as shown in table 2.5. This is to ensure that the alarms received are from more than one neighbor (ALARM_THRESHOLD) for subsequent actions.

Table 2.4: Trust Reply Table

Dest. Node Id	(Trust Reply 1)		(Trust Reply 2)		...		(Trust Reply N)	
	Node Id	Trust Value	Node Id	Trust Value	Node Id	Trust Value	Node Id	Trust Value

Table 2.5: Alarm Node Trust Table

Malicious Node Id	Count

2.2 Trust based Routing Protocol

This section describes the proposed trust based routing protocol in the MANET architecture. The protocol has two mechanisms, namely, route discovery and route maintenance.

2.2.1 Route Discovery

Figure 2.1 shows the route discovery mechanism. The undirected lines in figure 2.1 represent wireless communication link between the nodes. The steps for route discovery are as follows.

2.2.2 Route Maintenance

When a link break occurs in an active route, the node upstream of that break chooses to repair the link locally if it is closer to the destination. To repair the link break, the repairing node broadcasts a RREQ message for the destination. Since such RREQ message is in response to local link repair, it does not warrant being through $ATMn$ of the repairing node. If the repairing node receives a RREP then the route is locally repaired, otherwise it transmits a route error (RERR) message to its precursors. When the source node receives the RERR message, the source node rediscovers the route.

2.2.3 Dealing with Malicious Nodes

Since ongoing communications are tapped by nodes, behavior of neighboring nodes get reflected into their node trust table by using equation (2.1). A node broadcasts an alarm message (TREP with alarm) if it detects a node with trust value below a threshold (NODE_TRUST_THRESHOLD) as malicious. Nodes use alarm node trust table and ALARM_THRESHOLD to deal with malicious nodes. Algorithm 1 gives an abstract procedure to deal with malicious nodes in the proposed trust based routing protocol.

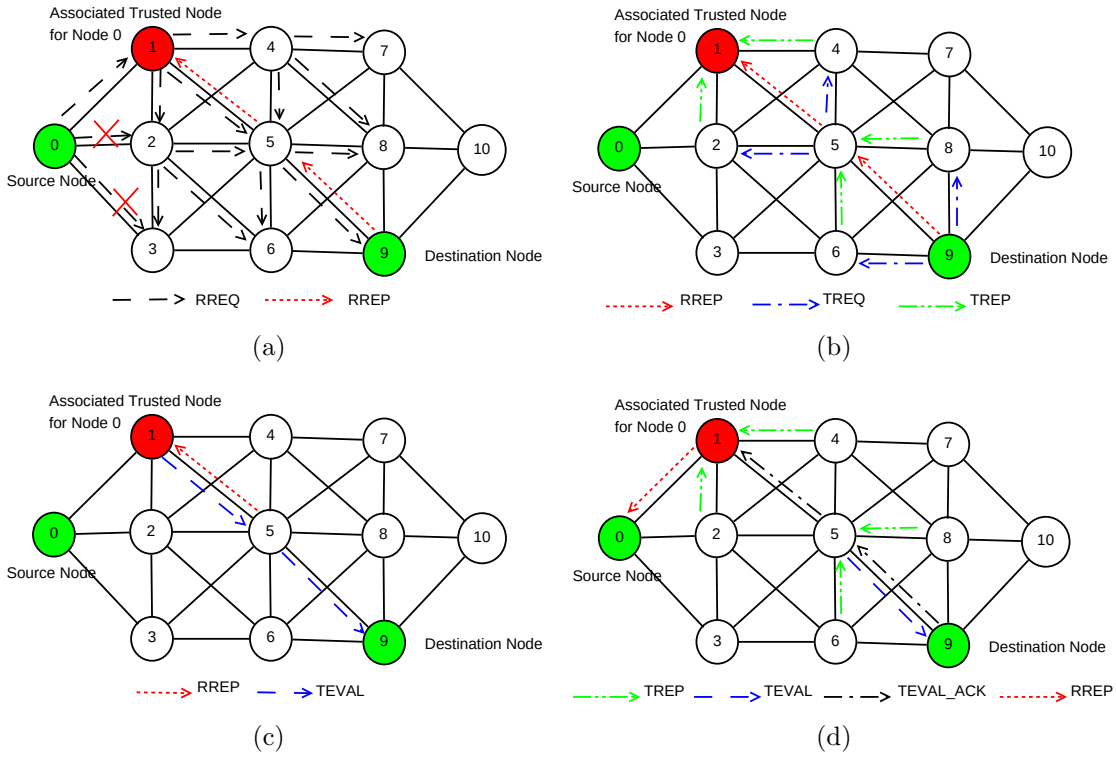

Figure 2.1: Trust based routing (a) Route Request (RREQ) and Route Reply (RREP) (b) Route Reply (RREP), Trust Request (TREQ) and Trust Reply (TREP) (c) Route Reply (RREP) and Trust Evaluate (TEVAL) (d) Trust Evaluate Acknowledgment (TEVAL_ACK) and Route Reply (RREP)

2.2.4 Simulation Environment and Parameters

Nodes are randomly distributed in an area of size 1000 m×1000 m using scene generator of Ns2. Every node chooses one of the neighbors with the highest trust value and lowest index/ID as its *ATMn*. The experiments are conducted on Constant Bit Rate (CBR) data traffic using traffic generator of Ns2 with a packet size of 512 bytes and packet interval of 0.1 sec. Table 2.6 shows the topology related parameters in Ns2. Table 2.7 shows the characteristics of CBR traffic.

Table 2.6: Topology Related Parameters

Parameter	**Value**
Number of Nodes	200
Radio Range	250 m
Available Bandwidth	2 Mbps
Area	1000 m×1000 m
Simulation Time	100 sec

Algorithm 1 Dealing node

Require: Id (Node ID of malicious node), Current_Node_Address (Node ID of current node)

```
1: if NodeTrustTable[Id].Value < NODE_TRUST_THRESHOLD then
2:    Aflag = 1
3:    SRC = Current_Node_Address
4:    DST = Id
5:    Broadcast TREP with hopcount as 1
6: end if
7: if TREP then
8:    if Aflag == 1 then
9:       Alarm_NodeTrustTable_insert(TREP.DST)    {Alarm count incremented for the
         DST}
10:   end if
11: end if
```

Table 2.7: CBR Traffic Characteristics

Parameter	**Value**
Packet Size	512
Packet Interval	0.1 sec
Max. Packets	10000

2.2.5 Performance Metrics

Performance metrics used for the analysis are Packet Delivery Ratio (PDR) and Control Traffic Overhead (CTO). PDR is computed as ratio of data packets delivered to packets generated.

$$PDR = \left(\frac{\text{data packets delivered}}{\text{data packets generated}} \right)$$

CTO is computed as control routing bits transmitted per data bits transmitted, i.e., ratio of sum of total RREQ, RREP, RERR, TREQ, TREP, TEVAL, and TEVAL_ACK overheads to total data bits transmitted.

$$CTO = \left(\frac{\text{total control routing bits transmitted}}{\text{total data bits transmitted}} \right)$$

Performance is compared in same topology, parameters, traffic and (source, destination) pair.

2.2.6 Experimental Results and Discussion

Figure 2.3 shows performance comparison under varying total number nodes in the network topology. The results are drawn from an average of 20 test runs. Figure 2.3(a) shows

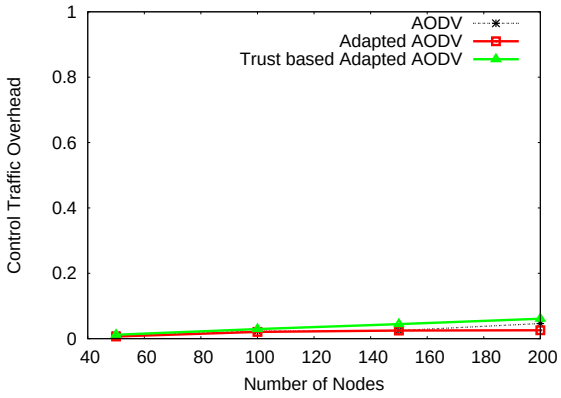

Figure 2.2: Performance Comparison Packet Delivery Ratio

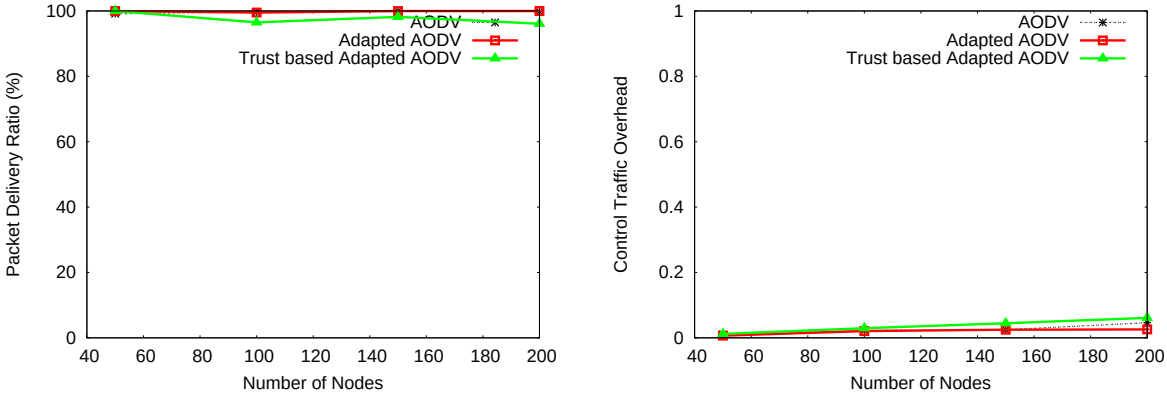

Figure 2.3: Performance Comparison (a) Packet Delivery Ratio (b) Control Traffic Overhead

that, PDR of Trust based Adapted AODV is at par with that of Adapted AODV and AODV. However, there is an increase in CTO than that of Adapted AODV and AODV (in figure 2.3(b)).

Figure 2.4 shows the performance comparison of Trust based Adapted AODV and Adapted AODV for CBR traffic in the presence of malicious nodes. In the simulation, CBR traffic is started at 5 sec, and packet dropping by malicious nodes are started at 20 sec in a simulation time of 50 sec. Figure 4(c) shows number of packets dropped in Adapted AODV and in Trust based Adapted AODV. Figure 4(d) shows path rediscover time when the nodes do not have sufficient trust related information and the time is calculated from the time nodes start misbehaving.

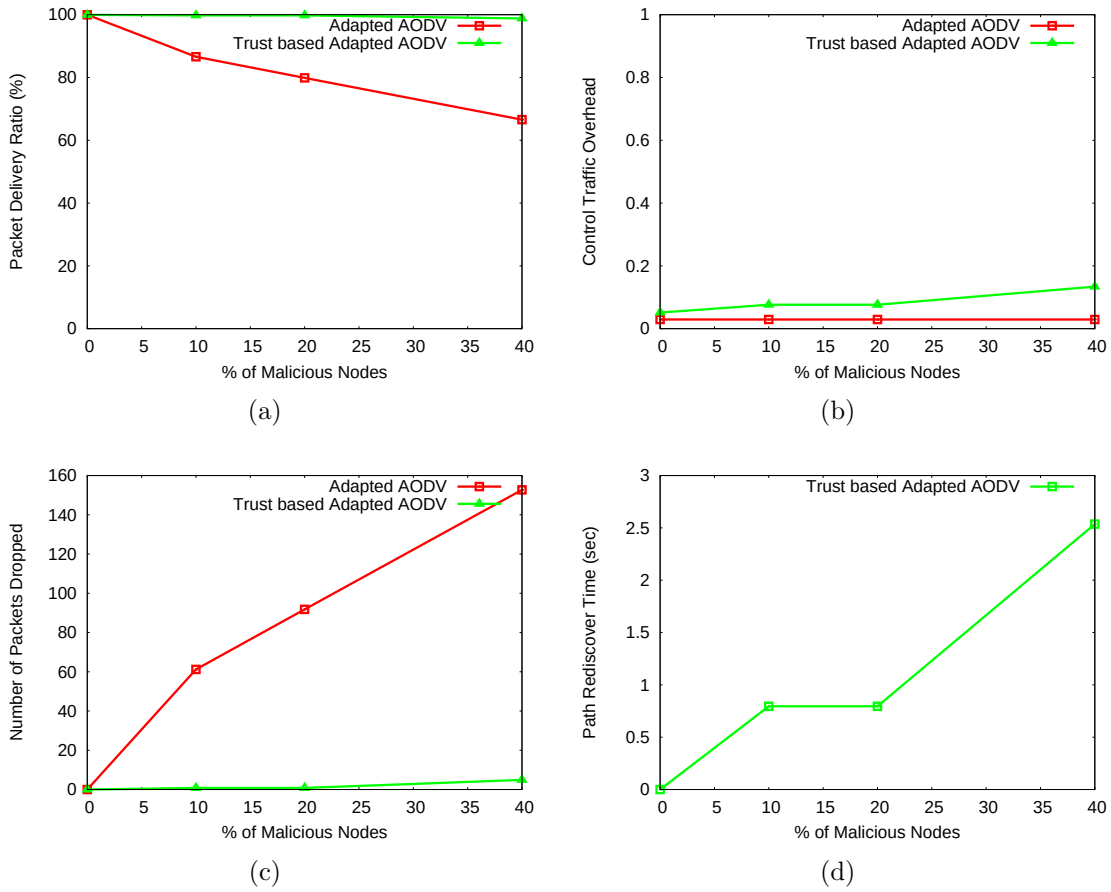

Figure 2.4: Performance Comparison in the Presence of Malicious Nodes (a) Packet Delivery Ratio (b) Control Traffic Overhead (c) Packets Dropped (d) Path Rediscover Time

2.3 Summary

In this chapter, a trust management scheme based on reputation, recommendation and context has been presented. However, all communications in the MANET are exposed and prone to unauthorized access. Next chapter presents key management scheme.

Chapter 3

Conclusion and Future Work

Appendix A

Disasters in India

Bibliography

[1] C. T. Butts and M. Petrescu-Prahova, "Radio communication networks in the world trade center disaster," http://gladiator.ncsa.uiuc.edu/PDFs/networks/butts-radio.pdf, Apr 2005.

[2] S. S. Kulkarni, M. G. Gouda, and A. Arora, "Secret instantiation in ad-hoc networks," *Computer Communications*, vol. 29, no. 2, pp. 200–215, 2006.

[3] C. K. Wong, M. Gouda, and S. S. Lam, "Secure group communications using key graphs," *SIGCOMM Comput. Commun. Rev.*, vol. 28, no. 4, pp. 68–79, 1998.

Index