CHAPTER VI

PERFORMANCE ANALYSIS OF RESEARCH WORK

6.0 INTRODUCTION

Recently, various researches have focused on building up trust among distributed network nodes to simulate co-operation and improving the performance and security of the network. Multiple evidences should be used in the trust evaluation of the node, so the different levels of importance for all of the evidences and characteristics should be taken into account, we need to use different weights to indicate the relative importance of different evidences. In MANETs, a trust relationship formed from direct interactions can be characterized as a direct trust; a trust relationship or a potential trust relationship built from recommendations by a trusted node or a chain of trusted nodes, which create a trust path, is called indirect trust [43].

The hypothesis that nodes with the high TV will give honest recommendations is questionable. The trust model in a MANET environment is hard to assess due to the uncertainties involved. The theory of fuzzy logic extends the ontology of mathematical research to be a composite which leverages quality and quantity, and which contains certain fuzziness. Introducing fuzzy logic into the research of trust management by combining the collaborative filtering, we try to
solve the issues associated with uncertainty in a MANET trust management.

Research in the area of service discovery for ad hoc networks is relatively new. Solutions [23], [41] primarily utilize the broadcast-driven nature of the underlying ad hoc network to carry out service discovery. We have shown in Chapter 5 that broadcast-driven protocols do not work well in terms of scalability and efficiency of discovery for large scale pervasive environments. There has been work in the field of wired networks to develop server-less peer-to-peer architectures as shown in [1], [4], [7].

6.1 METRICS

The following metrics are considered:

Throughput / Latency: The total throughput of a network with n mobile nodes [6]. That is, the data forwarded to the correct destination for each node i is denoted as follows:

\[ \text{Throughput} = \frac{\sum_{i=1}^{i=N} P_{\text{recv}}}{\sum_{i=1}^{i=N} P_{\text{origin}}} \]

PDR (Packet Delivery Ratio): This measures the quality of the recommended model, and it denotes statistical accuracy and decision support accuracy for trust recommendation in MANETs. MAE is one of the statistical accuracy metrics.
\[ \text{MAE} = \frac{\sum_{i=1}^{N} |T_{ri} - R_{ri}|}{N} \]

Here the set of trust recommendation is \((tr_1, tr_2, ...tr_n)\) and the set of real evaluations is \((Rr_1, Rr_2, ...,Rr_n)\).

### 6.2 PERFORMANCE ANALYSIS

The research work is categorized into three modules - PROFIDES using a simple traffic behavior markovian modeling approach [1], which classifies data / control packets using profile based mining method. This scheme significantly identifies intrusion of MANET nodes during session connectivity established between nodes. The second work, TRUCE depends on trust establishment between a cluster domain of nodes in activity using key exchange between set of nodes. Third work TUFY, which adapts distributed fuzzy approach over Trust establishment between mobile nodes with different service capabilities.

The three security schemes were found to be scalable to increasing number of mobile nodes and varying type of services. Experimental test beds were conducted using ns2 simulator and real time test setups as discussed in Chapter 3, Chapter 4 and Chapter 5. The performance analysis of schemes can be summarized as below:

1. Both TRUCE and TUFY without pubic key verification are vulnerable to impersonation attacks. The impacts of these two
security schemes are similar, where more the number of malicious nodes in the network is, then lesser the number of data packets is received.

2. As shown by the experiments, TRUCE is secure against impersonation attack only when there is a way to verify the public key of the route reply originator. In other words, a key control management center is required to make TRUCE secure against impersonation attacks, which is an outstanding issue compared to TUFY and PROFIDES.

3. PROFIDES security scheme works better in case of large traffic overhead whereas TRUCE and TUFY highly depends on number of sessions being maintained.

4. TUFY adapts to varying mobile node service capability and differing bandwidth requirements, where TRUCE and PROIFDES are not specifically dependent on service type.

To identify the performance of PROFIDES, TRUCE and TUFY over feasible routing protocols AODV, CONFIDANT, test bed was conducted using ns2 simulator.
Fig. 6.1 Performance analysis over PROFIDES, AODV, CONFIDANT, TRUCE and TUFY

Fig. 6.1 shows the performance analysis of PROFIDES, TRUCE and TUFY security schemes in comparison with MANET security scheme CONFIDANT and QAODV (Quality of Service Ad hoc On-demand Distance Vector) implemented based on research outcomes.

Fig. 6.1a, shows the performance of proposed security schemes over a simulated test bed using 1800 stream bytes of data. It can be identified that

[a] Bandwidth used for TUFY is optimally higher hence minimal latency is achieved.

[b] TRUCE shows Minimal delay with minimal bandwidth in use.

[c] CONFIDANCE acquires optimal bandwidth but latency is found to be higher due to higher number of hops and higher RTT.
[d] AODV represents a higher delay, high number of hops and percentage of packet loss hence high latency.

Fig. 6.1b, shows the performance of proposed security schemes over a simulated test bed using 2400 stream bytes of data. It can be identified that:

[a] Even though bandwidth utilized is higher than optimal, number of hops higher, loss is minimal due to traffic control at gateways for PROFIDES.

[b] TRUCE observes Optimal bandwidth utilized at each gateways, with minimal number of hops and minimal RTT, minimal Delay hence minimal latency.

[c] CONFIDANT shows high latency due to high percentage of data loss at gateways, even though it consumes minimal number of hops.

[d] AODV utilizes high bandwidth, higher RTT, higher delay hence higher latency.

Fig. 6.1c, shows the performance of proposed security schemes over a simulated test bed using 2200 stream bytes of data. It can be identified that:

[a] TRUCE supports minimal number of hops, minimal RTT, hence minimal latency.

[b] TUFY demonstrates minimal hops, bandwidth optimized, minimal loss and latency minimal.

[c] PROFIDES consumes higher delay.

[d] CONFIDANT consumes higher bandwidth due to maximal number of hops, high RTT and percentage of loss.
Fig. 6.1d, shows the performance of proposed security schemes over a simulated test bed using 2300 stream bytes of data. It can be identified that:

[a] **TRUCE** behaves with higher delay when compared with **PROFIDES** but consumes minimal bandwidth.

[b] **TUFY** absorbs optimal bandwidth with minimal percentage of loss compared to other schemes, hence displays minimal latency.

[c] **PROFIDES** supports minimal number of hops, but higher percentage of loss and hence moderate latency effect.

[d] **AODV** has high latency due to high percentage of loss and high number of hops and high delay.

From the test-bed and demonstration it can be identified that, **PROFIDES** behavior is found to handle effective intrusions based on traffic behavior of nodes while the performance of **TRUCE** and **TUFY** is found to be effective in terms of mean error rate (latency), number of hops, **RTT** and optimal bandwidth utilization.