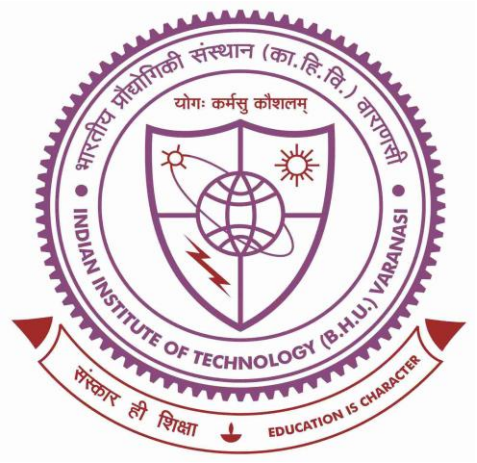
Performance Analysis of MANETs Routing Protocols with Disaster Application and Security Issues



THESIS SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENT FOR THE AWARD

OF

Doctor of Philosophy

in

Systems Engineering

Supervisor
Dr. Suresh C. Gupta
Professor

Submitted by
Ashutosh Srivastava

DEPARTMENT OF ELECTRICAL ENGINEERING
INDIAN INSTITUTE OF TECHNOLOGY
BANARAS HINDU UNIVERSITY
VARANASI–221 005, INDIA

Enrolment No. 302124

April-2016

Chapter 7

Conclusions

Mobile Ad Hoc Networks are infrastructure less, decentralized, dynamic and multi hop networks composed of bandwidth constrained wireless links and no centrally accessed servers. There performance is affected by choice of routing, terrain features, mobility, mobility models framework etc. Performance is estimated in terms of the metrices like Packet delivery ratio or fraction, End to End delay, Throughput or Goodput, Jitter etc. The Study of MANET scenarios and applied parameters are important to select appropriate routing protocols from the right group of protocols for any application. Analysis and conclusions may prove to be useful while selecting routing protocols for MANET applications.

We first compared the two commonly used simulators NS2 and Qualnet for routing protocols namely AODV (reactive) and OLSR (proactive). It was observed that NS2 has scalability issues when the network size exceeds 500, which confirms the study in [7]. In chapter 3, we have compared essential features of Network simulators including NS2 & Qualnet. We investigated performance and scalability of the tools. Then for examine purpose same set of conditions were employed on two simulators. Our result shows that both Ns2 and Qualnet are efficient for carrying out small-scale network simulations; however for a moderate scaled network Qualnet performs better regarding network speed, memory consumption and for larger areas.

In the next section we evaluated a proposed layered framework model for post disaster situation. We have simulated mobility framework with three routing algorithms ZRP, AODV, and OLSR. Our simulation shows that routing algorithms behave significantly different under the mobility scenarios designed on the same platform. For analyzing the performance of routing protocols, a scenario based approach is vital. We also conclude that by organizing the terrain region into four equal sized symmetrically placed sub-regions, we obtain optimum results in the terms of PDF, end-to-end delay, normalized routing load, and data packets forwarded.

In chapter 5, the issue of packet drop in MANETs was tackled, Packet drop may occur due to link errors because of interference or fading. Packet-dropping attack has always been a significant threat to the security in MANETs. In this chapter, we have described

and simulated the DSSAM method in a standard environment and compared it with existing methods under different scenarios. The obtained simulation outcome provides enhanced performance against watchdog and TWOACK in the cases of receiver collision, limited transmission power, and false misbehavior acknowledgment. We incorporated digital signature in the method. Even though it generates more routing overhead in few cases but there was a performance improvement in packet delivery fraction. We have considered two cases. In the first case, malicious nodes drop all the packets. Our proposed method DSSAM outperforms Watchdog's performance by average of 20% when there are 20% of malicious nodes in the network. From the results, we observe that acknowledgment-based schemes, including TWOACK and DSSAM, are able to detect misbehaviors with the presence of receiver collision and limited transmission power. However, when the number of malicious nodes reaches above 40%, our proposed scheme DSSAM's performance is better than others.

In the second case, we seeded malicious nodes which send fake acknowledgement to the source node. This was done to check the intrusion detection systems performance under fake acknowledgement. When the percentage seeding of malicious nodes is 10%, the performance of DSSAM is about 3% better than TWOACK. When the malicious nodes are at 20% and 30%, DSSAM outperforms all other schemes.

In Chapter 6 application demands optimize and concise way for covering all permanent check positions with obstacle avoidance. It also requires an exchange of real-time information among responders for saving lives. Here mobility of MANET nodes between stages has been modeled with "SROA" (Shortest route with obstacle avoidance) shortest route from Source to destination covering all checkpoints (here in levels there are defined checkpoints) with obstacle avoidance mechanism. We observe the performance of SROA and RWP mobility method on average links broken for the same terrain. The average number of links broken on node speed and transmission range at the time of simulation was evaluated to determine the impact of the obstacles and pathways.

There is tremendous scope of studying and analyzing performance of MANETs, to match these and several exciting newer areas of their applications- UAV Networks, VANET, Sensor Networks, Robotics Networks etc. It is therefore likely to continue as important areas of research and development.