Jamming-Resilient Secure Neighbor Discovery In Mobile Ad Hoc Networks

S.Jayashree [1]D.K.Indhu[2]M.Shilpa[3]

Abstract*—*JR-SND, a jamming-resilient secure neighbor discovery scheme for MANETs based on direct-sequence spread spectrum and random spread-code predistribution. JR-SND enables neighboring nodes to securely discover each other with overwhelming probability despite the presence of omnipresent jammers. It considers the energy consumption and the remaining battery energy of nodes as well as quality of links to find energy-efficient and reliable routes that increase the operational lifetime of the network. HDSR, on the other hand, is an energy-efficient routing algorithm which finds routes minimizing the total energy required for end-to-end packet traversal. HDSR are proposed for networks in which either hop-by-hop or end-to-end retransmissions ensure reliability.

I. INTRODUCTION

A key feature of mobile ad hoc networks (MANETs) is that information can be routed from a source node to a destination node even if the two are not directly connected via a physical link. Information is routed via other intermediate nodes, where routes are established in MANETs using one or more routing protocols. One popular MANET routing protocol is optimized link state routing (OLSR) [2]. With OLSR, every node proactively maintains routing tables to destination nodes so that information packets can be routed on existing routes, as opposed to establishing routes on-demand. The tables are established and maintained by periodic 'hello' and 'topology control' protocol messages. The focus of this paper is on 'hello' messages, which have a short period and are exchanged to establish two-hop connections, an essential step in the protocol. According to the OLSR standard [2], a random jitter value is subtracted from the period of 'hello' messages in order to avoid synchronization of messages among nodes and reduce the probability of message collisions. The 'topology control' messages have a longer period than 'hello' messages and are broadcast by multipoint relay (MPR) nodes that are selected to extend the reach of a node beyond two hops.

As mentioned earlier, the OLSR standard indicates that the jitter should be randomly generated. However, we observed from laboratory network captures of physical layer (PHY) messages that in the commercial devices we studied, the jitter
values are not purely random. This observation can be used to gradually put the OLSR protocol under denial of service (DoS) with resulting degradation on link availability. In this work, we investigate how this non-random jitter can be exploited to deny service to the OLSR protocol. We further explore how DoS on the OLSR protocol affects MANET performance.

We consider two metrics for evaluating network performance under interference: mean time between failure (MTBF) is a measure of 'link availability' and 'percent connectedness' is defined as percentage of time a connection exists in the link. We use these metrics to evaluate the robustness of the OLSR protocol when the 'hello' messages are targeted by unwanted interference. We discuss that a random jitter in 'hello' message periodicity is important for OLSR's robustness and ultimately for a MANET's resilience against denial or degradation if its routing protocol were targeted.

In section II, we provide a short overview of different types of jammers found in the literature for targeting a periodic protocol. In section III we present excerpts from the OLSR protocol about the periodicity, jitter, and duration of a typical 'hello' message and present our observations from two data sets recorded using different commercial off-the-shelf (COTS) hardware. We present an algorithm in section IV that uses OLSR 'hello' statistics to predict the next 'hello' message and put the OLSR protocol under increasing DoS. We present performance results of our simulations in Section V followed by concluding remarks in section VI.

II. OVERVIEW OF PROTOCOL JAMMERS

In MANETs, robust routing via intermediate nodes is at the mercy of the wireless medium. In this section we present a short overview of different types of jammers found in the literature that target wireless signals carrying protocol messages.

Wireless signals can be degraded, even disabled, by jamming techniques where co-channel interferers disrupt the integrity of the received signal [4]. High power transmission of continuous-wave signals within radio range of a target can reduce the signal-to-noise ratio of the target to an unusable level [5], but this method of jamming could also lead the jammer to be detected, located, and removed [6]. As an alternative, a smart jammer only transmits when it senses channel activity. As another alternative, a sophisticated smart jammer only transmits when it senses channel activity of the type targeted, e.g., messages of a targeted communication protocol. Such a jammer, also known as protocol jammer

III . EXISTING SYSTEM

The existing solutions all depend on some publicly known communication strategies such as public spread-code sets. The adversary can thus use such public knowledge to inject arbitrary many neighbor discovery requests in the whole network, leading to a special Denial-of-Service (DoS) attack in which all nodes are forced to perform endless verifications of neighbor discovery requests (which often involve expensive digital signature verifications).

DISADVANTAGES

- Existing approaches are not scalable
- They not cover group communication.

IV. PROPOSED SYSTEM

We propose resent advances in trust management scheme that enhances the security in MANET. In the trust management scheme we use hybrid dynamic secure routing protocol (HDSR) it has two components: Trust value in direct observation and trust value in indirect observation. In direct observation the trust value is derived using Bayesian inference and indirect observation the trust value is derived using dempster- Shafer theory.Indirect observation is also called as second hand information, it is obtained from neighbor node of the observer node. Combining these two components we can get accurate trust value. Simulation result show that throughput and packet delivery ratio will be improved and reduce end to end delay and overhead of messages.

ADVANTAGES

- Throughput and packet delivery ratio can be improved significantly, with slightly Reduced average end-to-end delay and Routing overhead of messages.

V. HARDWARE CONFIGURATION

Processor : Intel Pentium Iv

Hard Disk Space : 40gb

Monitor : 14''

Printer : Hp 1020

Keyboard : 104 Keys

Internal Memory Capacity : 256 Mb

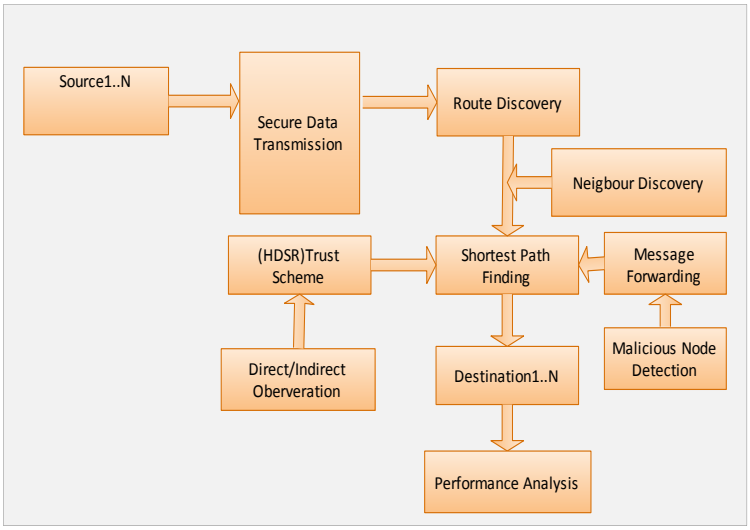
Mouse : Optical Mouse

VI.SOFTWARE CONFIGURATION

Software: Ns-2

Language: Object Oriented Tool Command Language (Otcl)

VII.FLOWDIAGRAM



VIII. LIST OF MODULES

- **1.Network Deployment**
- **2.Data Communication**
- **3.HDSR**
- **4.Performance Analysis**

1.NETWORK DEPLOYMENT:

Mobile ad hoc network is composed of several mobile nodes, all the nodes are deployed in an area for a particular purpose.

2. DATA COLLECTION AND AGGREGATION

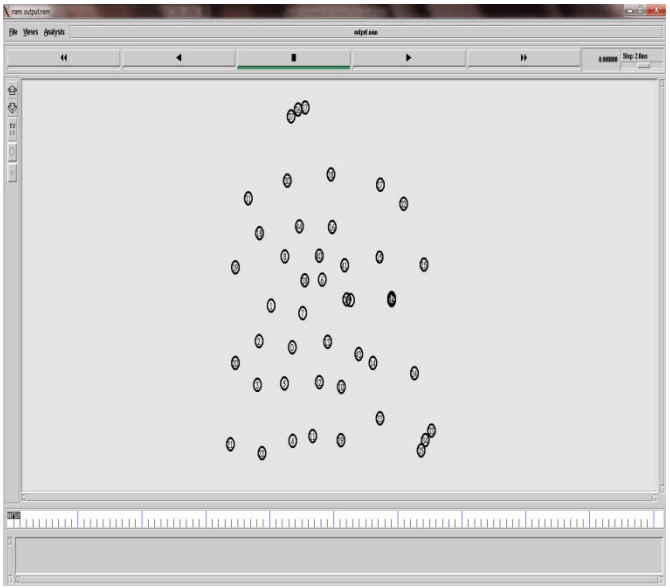
3. HDSR

It propose resent advances in trust management scheme that enhances the security in MANET. In the trust management scheme we use hybrid dynamic secure routing protocol (HDSR) it has two components: Trust value in direct observation and trust value in indirect observation. In direct observation the trust value is derived using Bayesian inference and indirect observation the trust value is derived using dempster-shafer theory. Indirect observation is also called as second hand information.

4. PERFORMANCE ANALYSIS

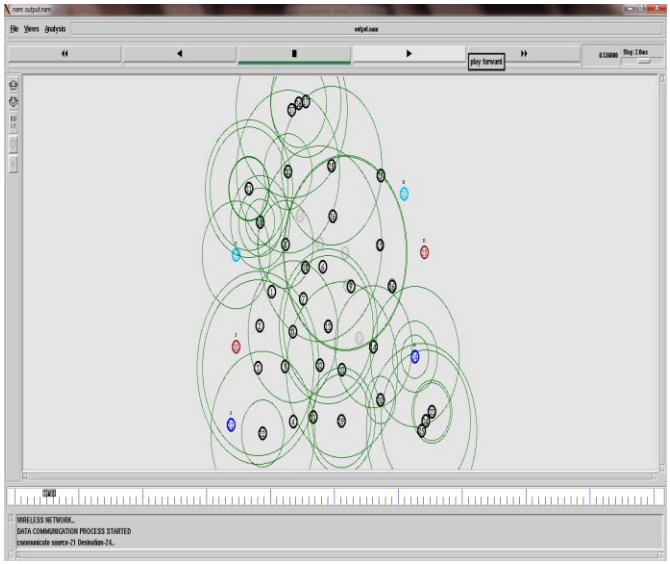
This module is developed to improve mobile ad hoc network performance, Reduce Average end –to-end delay.

NETWORK DEPLOYMENT



DATA COMMUNICATION

This Module is developed to MANET networks data communication and aggregation process. The radio and IEEE 802.11 MAC layer models were used. The network based data processing are most expensive and data communication level on their performance on the network. Multiple sources create and end sending packets; each data has a steady size of 512 bytes. Each node to move randomly on their network, it's more and most expectable on their networks.



IX. CONCLUSION

Finally, it propose resent advances in trust management scheme that enhances the security in MANET. In the trust management scheme we use hybrid dynamic secure routing protocol (HDSR) it has two components: Trust value in direct observation and trust value in indirect observation. In direct observation the trust value is derived using Bayesian inference and indirect observation the trust value is derived using dempster-shafer theory. Indirect observation is also called as second hand information

X. REFERENCES

1. H. Wang, L. Zhang, T. Li, and J. Tugnait, "Spectrally efficient jammingmitigation based on code-controlled frequency hopping," *IEEE Trans.Wireless Commun., vol. 10, no. 3, pp. 728–732, Mar. 2011*
2. R. Pickholtz, D. Schilling, and L. Milstein, "Theory of spread-spectrumcommunications-A tutorial," *IEEE Trans. Commun., vol. COM-30, no. 5,* pp. 855–884, May 1982.
3. P. Papadimitratos*et al., "Secure neighborhood discovery: A fundamental*element for mobile ad hoc networking," *IEEE Commun. Mag., vol. 46,*no. 2, pp. 132–139, Feb. 2008

4. L. Xiao, H. Dai, and P. Ning, "Jamming-resistant collaborative broadcast using uncoordinated frequency hopping," *IEEE Trans. Inf. Forensics Security, vol. 7, no. 1, pp. 297–309, Feb. 2012*