ADAPTIVE MANET ON THE SCENARIOS AND MINIMIZING THE GREY-HOLE DOS ATTACK

Dr.R,ManiKandan[1], k.Vijayalakshmi[2]
[1]Assistant Professor / Programmer,
Department of Computer Science And Engineering,
Government College Of Engineering-Dharmapuri.
rmkmanikandan@yahoo.co.uk
[2]Lecturer, Computer Science and Engineering,
Srinivasa Subbaraya Government Polytechnic College, Puthur-609108
mailtovijius@gmail.com

ABSTRACT

Mobile ad hoc networks (MANETs) are generally created for temporary scenarios. In such scenarios, where nodes are in mobility, efficient routing is a challenging task. In this paper, we propose an adaptive and cross-layer multipath routing protocol for such changing scenarios and a method for minimizing the gray-hole DoS attack. Our solution assumes no explicit node collaboration, with each node using only internal knowledge gained by routine routing information. In case of multimedia applications, the proposed mechanism considers such routes which are capable of providing more data rates having less packet loss ratio. For those applications which need security, the proposed mechanism searches such routes which are more secure in nature as compared to others. The average remaining energy, network throughput, packet loss probability, and traffic load distribution are improved by about 10%, 10%, 5%, and 10%, respectively, more than the existing schemes. Our simulation results show a decrease of up to 51% in previously dropped packet, greatly minimizing gray-hole attack effectiveness.

1. Introduction

Mobile ad hoc networks (MANETs) are composed of different nodes being operated in infrastructureless environment. These nodes work in a highly dynamic and random topology [1]. Nodes are distributed and mobile with the capability of self-organizing themselves. MANET nodes have resource constraints such as power, processing, and bandwidth. Comparing with the traditional network, MANET inherits the traditional problems of wired and wireless network. Its basic infrastructure less features imposes another burden on the standardization of network architecture. To compare with that of traditional networks, wireless network security must address two foundation aspects. One is key management, trust establishment, and membership control; the other one deals with network availability and routing security.

Proactive or table driven routing protocol [3–8] established paths in their routing table before they are required. Nodes operating under proactive protocol continuously propagate routing related information to their neighbors to update their routing table. This process is periodic in nature. Therefore, a source node before transmitting any data packet gets the full path in advance. In case of any link changes, respective nodes update their routing table by doing the same exchange of information process. The advantage of using proactive approach is quite straightforward; that is, the nodes get the full path in advance. The disadvantage is that nodes are always busy in computing their routing table and network overhead is large. Some of the popular proactive protocols are WRP (Wireless Routing Protocol), DSDV (Destination Sequence Distance Vector), FSR (Fisheye State Routing), and so forth.

Some of the major routing protocols that fall into the category are AODV (ad hoc on-demand

distance vector) and DSR (Dynamic Source Routing), and so forth.

The reminder of this paper is organized as follows. In Section II-A the OLSR protocol is presented; then, the grayholeattack is described. In Section II-C we briefly present the DCFM algorithm. The method for protecting OLSR MANETfrom gray-hole attack using DCFM is described in Section III. Section IV describes the simulation model and presents the results achieved along with a discussion of the results. Previous works related to OLSR security as well as to the grayhole attack are discussed in Section V. Finally, conclusions and future works are presented in Section VI.

2 Related works

Some serious research has been carried out in MANET different aspects, ranging from routing, energy management, to security requirements, and so forth. MANET basic goal is to work in multihop fashion so that intermediate nodes forward packets to the destination. Therefore, intermediate nodes play an important role in MANET. Availability is the main focus in the overall performance of the network, which demands efficient routing mechanism for MANET. Once all paths are discovered, source node selects one path to send the datagram packet to the destination. This single path selection is mostly done on the basis of shortest path. Shortest path generally follows the Bellman-Ford Algorithm, for example, OLSRBF [28]. The problem with the shortest path is that every node in the MANET will probably choose that path. This might become the center point of communication in most cases and more traffic passes through it. As a result more traffic yields more congestion and more delay [29]. This problem is solved by multipath routing.The proposed routing is adaptive in nature, that is, keeping in view the nature of the application; it selects two or more routes from source to destination. There is one default path, while other paths are based on available data rates, end-to-end delay, and security. Cross-layered mechanisms are used to exchange parameters across different layers. The protocol is taking care of the following three scenarios:
(i)Two or more than two default routes.
(ii)Two or more than two routes for multimedia applications.(iii)Two or more than two secure routes for sensitive applications.

2.1Algorithm

Step 1. Each node dynamically estimates the d, $\mathscr{C}$, E, $\Theta(\cdot)$, $\Psi(\cdot)$, and α values based on the real-time measurement.

Step 2. The $L.P$ value is locally calculated according to (1).

Step 3. At the initial time for routing operations, the source node broadcasts the initial PC value to neighbor nodes. Each node calculates its PC value by using (4) and recursively forwards this information.

Step 4. Based on the PC value, route configuration process continues repeatedly until all available multipaths from the source to the destination node are configured.

Step 5. To transmit packets, each relay node temporarily selects a next relay node with the selection probability, which is estimated according to (5).

Step 6. If the N_{pc} value is higher than the C_{pc} (i.e., $N_{pc} - C_{pc} > 0$), the new selected neighbor node replaces the current relay node; proceed to Step 8. Otherwise, go to Step 7.

Step 7. When the N_{pc} value is less than the C_{pc} value (i.e., $N_{pc} - C_{pc} < 0$), a random number X is generated. If a generated X is less than the BP (i.e., $X < \mathrm{BP}$), the new selected neighbor node replaces the current relay node. Otherwise, the established routing route is not changed.

Step 8. In an entirely distributed fashion, this hop-by-hop path selection procedure is recursively repeated until the packet reaches the destination node.

3.Performance Evaluation

In this section, the effectiveness of the proposed algorithms is validated through simulation; we propose a simulation model for the performance evaluation. With a simulation study, the performance superiority of the proposed multipath routing scheme can be confirmed. The assumptions implemented in our simulation model were as follows.
(i)100 nodes are distributed randomly over an area of 500 × 500 meter square.
(ii)Each data message is considered CBR traffic with the fixed packet size.
(iii)Network performance measures obtained on the basis of 50 simulation runs are plotted as functions of the packet generation per second (packets/s).
(iv)Data packets are generated at the source according to the rate (packets/s), and the range of offered load was varied from 0 to 3.0.
(v)The bandwidth of the wireless link was set to 5 Mb/s and the unit_time is one second.
(vi)The source and destination nodes are randomly selected.
(vii)For simplicity, we assume the absence of noise or physical obstacles in our experiments.
(viii)The mobility of each mobile node is randomly selected from the range of 0–10 m/s, and mobility model is random way point model.
(ix)At the beginning of simulation, all nodes started with an initial energy of 10 joules.

(x)Three different traffic types were assumed; they were generated with equal probability.

Table 1 shows the traffic types and system parameters used in the simulation. Each type of traffic has its own requirements in terms of bandwidth and service time. In order to emulate a real wireless network and for a fair comparison, we used the system parameters for a realistic simulation model [21, 22].

Table 1: Type of traffic and system parameters used in the simulation experiments.

(a)

Traffic type	Bandwidth requirement	Connection duration (ave./sec)
I	128 Kbps	60 sec (1 min)
II	256 Kbps	120 sec (2 min)
III	512 Kbps	180 sec (3 min)

(b)

Parameter	Value	Description
unit_time	1 second	Equal interval of time axis
e_{dis}	1 pJ/bit/m^2	Energy dissipation coefficient for the packet transmission
E_{co}	10 nJ/bit	System parameter for the electronic digital coding energy dissipation
D_M	10 m	Maximum wireless coverage range of each node
E_M	10 joules	Initial assigned energy amount of each node
ω	1	The weighted factor for the trust level
I_T	10 seconds	The number of discrete times to estimate entropy
X	0~1	Generated random number

(c)

Parameter	Initial	Description	Values
α	1	The ratio of remaining to initial energy of node	0~1 (E_i/E_M)
$T(t)$	1	The ratio of remaining to initial packet amount at time t	0~1

Figure 1 compares the performance of each scheme in terms of the average remaining energy of wireless nodes. To maximize a network lifetime, the remaining energy is an important performance metric. All the schemes have similar trends. However, based on (1), the proposed scheme effectively selects the next routing link by considering the remaining energy information. Therefore, we attain much remaining energy under heavy traffic load intensities; it guarantees a longer node lifetime.

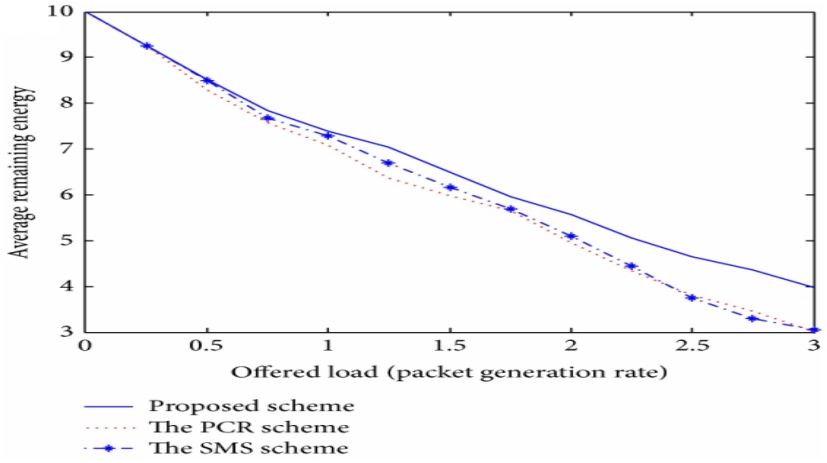

Figure 1: Average remaining energy.

Figure 2 shows the performance comparison of network throughput. Usually, network throughput is the rate of successful message delivery over a communication channel. The throughput is usually measured in bits per second (bit/s or bps) and sometimes in data packets per second or data packets per time slot. In this work, network throughput is defined as the ratio of data amount received at the destination nodes to the total generated data amount

.

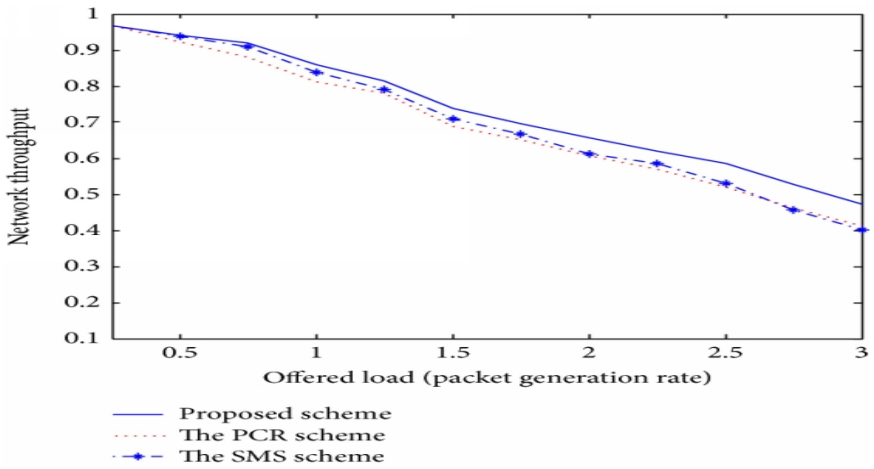

Figure 2: Network throughput.

In Figure 3, the packet loss probabilities are presented; packet loss means the failure of one or more transmitted packets to arrive at their destinations. As the offered traffic load increases, wireless nodes will run out of the energy or capacity for data transmissions and data packets are likely to be dropped.

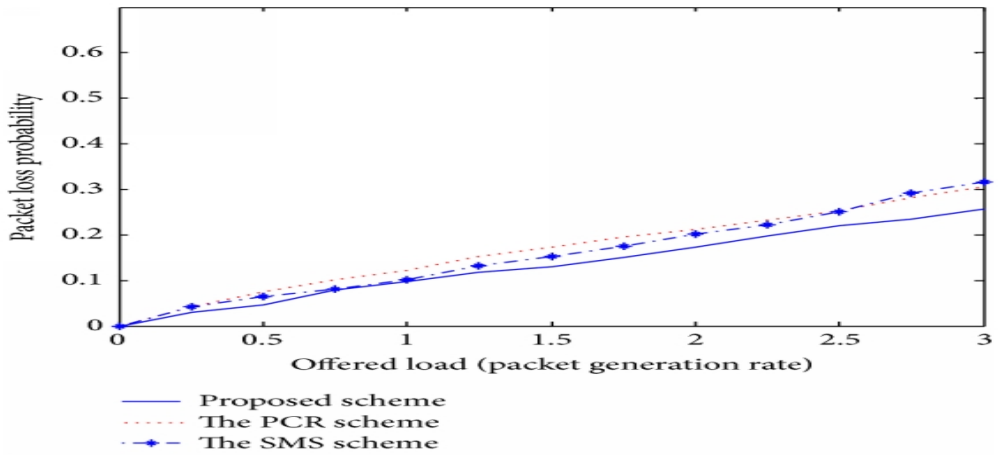

Figure 3: Packet loss probability.

The curves in Figures 4 and 5 indicate the average energy-exhaustion ratio and normalized traffic load distribution. In this paper, traffic load distribution means the average rate of traffic dispersion among wireless nodes. In an entirely distributed fashion, individual node in our scheme monitors the current network situation and updates all control parameters periodically for the adaptive routing.

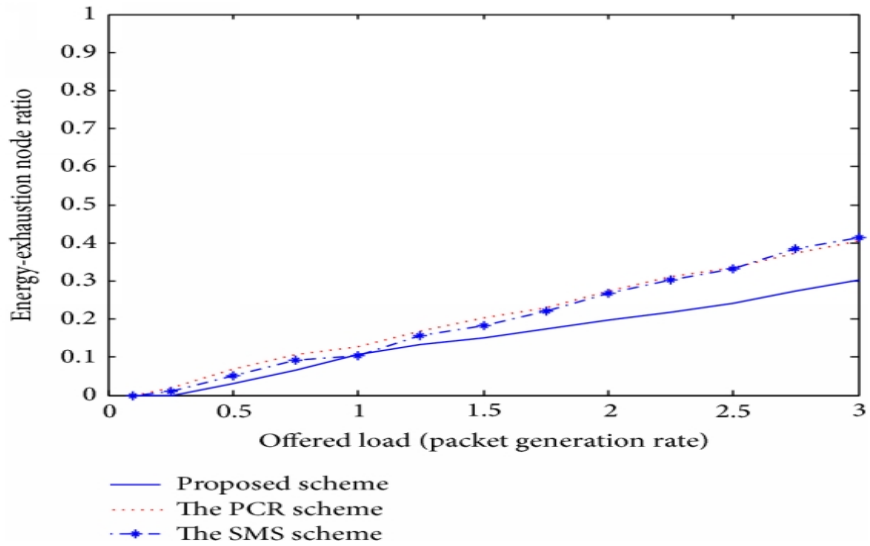

Figure 4: Energy-exhaustion ratio.

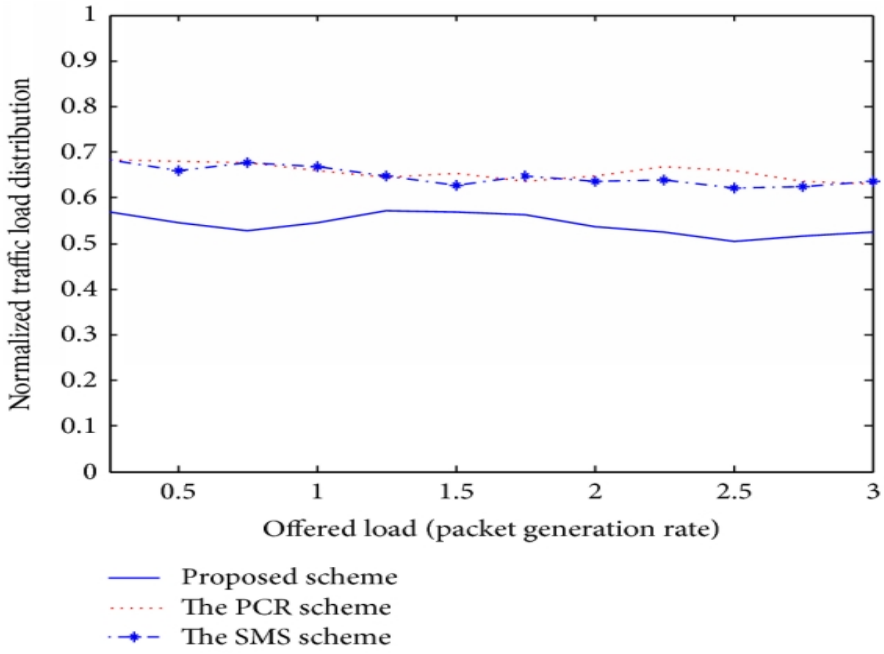

Figure 5: Normalized traffic load distribution.

4. Route Selection Process

Route selection process of the proposed scheme is discussed in detail in this section.

Default Route

Default routes will be searched if simple data needs to be transferred from source to destination; then two or more than two default routes are established between source and destination. These default routes will be the shortest routes among the available routes in terms of number of hops.

Considering the shortest route according to number of hops, the destination node will reply to the two most suitable routes, that is,

Route 2{n1,n7} ;

Route 3{n2,n7};

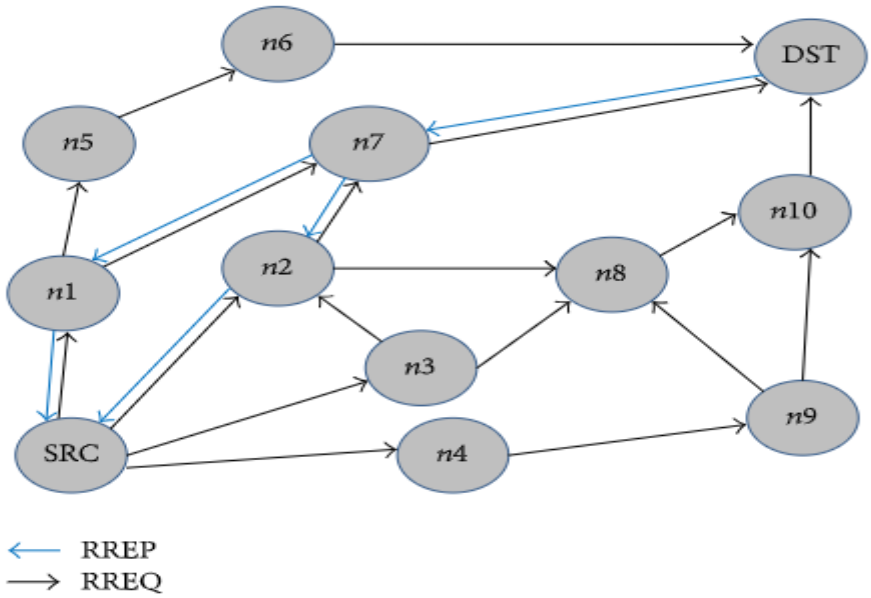

Figure 6: Path discovery process (default route).

Conclusions

In this paper, we presented cross-layer multipath routing protocol for MANET. The proposed protocol has two important features, that is, security and adaptive nature. These important features are achieved by multipath framework using cross-layer interface. Our proposed solution is capable of choosing multipaths by considering the type of application. The comparison covers most of the scenarios such as the packet delivery ratio, average delay, and routing overheads with and without malicious nodes. The proposed protocol is very effective in most of the scenarios that we tested.

References

1. L. Abusalah, A. Khokhar, and M. Guizani, "A survey of secure mobile Ad hoc routing protocols," IEEE Communications Surveys and Tutorials, vol. 10, no. 4, pp. 78–93, 2008.
2. R. Lacuesta, M. Garcia, J. Lloret, and G. Palacios, "Study and performance of ad hoc routing protocols," in Mobile Ad Hoc Networks: Current Status and Future Trends, pp. 71–101, CRC Press, Taylor and Francis, 2011.
3. C. E. Perkins and P. Bhagwat, "Highly dynamic Destination-Sequenced Distance-Vector routing (DSDV) for mobile computers," in Proceedings of the Conference on Communications Architectures, Protocols and Applications (SIGCOMM '94), pp. 234–244, London, UK, September 1994.
4. S. Murthy and J. Garcia-Luna-Aceves, "An efficient routing protocol for wireless networks," Mobile Networks and Applications, vol. 1, no. 2, pp. 183–197, 1996.
5. G. Pei, M. Gerla, and T.-W. Chen, "Fisheye State Routing: a routing scheme for ad hoc wireless networks," in Proceedings of the IEEE International Conference on Communications (ICC '00), pp. 70–74, New Orleans, La, USA, June 2000.
6. J. J. Garcia-Luna-Aceves and M. Spohn, "Source-tree routing in wireless networks," in Proceedings of the 7th International Conference on Network Protocols (ICNP '99), pp. 273–282, October-November 1999.
7. G. Malkin and M. Steenstrup, "Distance-vector routing," in Routing in Communications Networks, pp. 83–98, Prentice Hall, Englewood Cliffs, NJ, USA, 1995.
8. J. Moy, "Link-state routing," in Link-State Routing, Routing in Communications Networks, pp. 135–157, Prentice Hall, Englewood Cliffs, NY, USA, 1995.
9. C. E. Perkins and E. M. Royer, "Ad-hoc on-demand distance vector routing," in Proceedings of the 2nd IEEE Workshop on Mobile Computing

Systems and Applications (WMCSA '99), pp. 90–100, New Orleans, La, USA, February 1999.

10. D. Johnson, D. Maltz, and J. Broch, "DSR: the dynamic source routing protocol for multi-hop wireless ad hoc networks," in Ad Hoc Networking, pp. 139–172, Addison-Wesley, 2001.

11. C.-K. Toh, "Associativity-Based routing for ad-hoc mobile networks," Wireless Personal Communications, vol. 4, no. 2, pp. 103–139, 1997.

12. V. D. Park and M. S. Corson, "Highly adaptive distributed routing algorithm for mobile wireless networks," in Proceedings of the 16th IEEE Annual Conference on Computer Communications (INFOCOM '97), pp. 1405–1413, April 1997.