Path Hopping Based on Reverse AODV for Security

Elmurod Talipov, Donxue Jin, Jaeyoun Jung, Ilkhyu Ha,
YoungJun Choi, and Chonggun Kim*

Department of Computer Engineering,
Yeungnam University, Korea
elmurod@ynu.ac.kr, donghak@yumail.ac.kr,
e-mail@yumail.ac.kr, ilkyuha@yumail.ac.kr,
yjchoi@yu.ac.kr, cgkim@yu.ac.kr

Abstract. In Ad hoc networks, malicious nodes can enter in radio transmission range on the routing path and disrupt network activity. Therefore, protecting from intrusion of malicious node and enhance data security is an important issue on Ad hoc networks. In this study, we provide a path hopping method based on reverse AODV (R-AODV). By reverse AODV, source node builds multipath to destination and adaptively hops available paths for data communications. Hopping paths can protect data from the intrusion of malicious nodes. We propose an analytic method to expect intrusion rate and a path hopping routing mechanism to implement simulation models using NS-2.

Keywords: Path-hopping, reverse AODV, Ad hoc network security.

1 Introduction

A mobile ad hoc network is a dynamically self-organizing network without any central administrator or infrastructure support. If two nodes are not within the transmission range of each other, other nodes are needed to serve as intermediate routers for the communication between the two nodes [1, 2].

In ad hoc wireless networks, transmitted data is susceptible to potential attacks. Eavesdroppers can access secret information, violating network confidentiality. Hackers can directly attack the network to drop data packets, inject erroneous messages, or impersonate as a member node. To increase security, physical protection of the network from malicious node is important.

In this study we propose path hopping based on reverse AODV [2]. In R-AODV, which is an easy multipath searching method, destination node uses reverse RREQ to find source node rather than a unicast reply. It reduces path fail correction messages and also source node builds partial or complete non-disjoint multipath from source to destination. Hopping paths means source node sends each data packet through different paths each time, therefore eavesdropper will not get whole data and also its intrusion to network become harder [3-7].

Physical protection of data from malicious invader is an important security method. It can decrease or prevent packet loss by active malicious nodes [7].

* Correspondence author.

Y.-T. Kim and M. Takano (Eds.): APNOMS 2006, LNCS 4238, pp. 574 – 577, 2006.

2 Path Hopping Method on Multipaths

Path hopping based on reverse AODV routing protocol (PHR-AODV) is presented. Since PHR-AODV is reactive routing protocol, no permanent routes are stored in nodes. The source node initiates route discovery procedure by broadcasting the RREQ message. When destination node receives first route request message, it generates so called reverse request (R-RREQ) message and broadcasts it. By receiving R-RREQ messages source node simply builds partial non-disjoint multipath and hops one by one while sending data packets [2]. In PHR-AODV the number of paths from one source to destination is decided as the number of edges from source node.

Purpose of our study is to strength security of routing and decrease possible intrusions of malicious nodes. PHR-AODV maintains list of routing paths from source to destination. The messages are sent by multipaths. The order of path selection can be variable. We just accept sequential order in this study. During the communication, a path failed then the path is eliminated from the list. When no path is remained in the list, the source node sends RREQ for establishing new multipaths.

Path disjointing is an important point of multipath routing. Several disjointing paths are studied, such as [2], [5] and [7]. Generally multipath can be classified in three groups: node-disjoint (complete disjoint), link disjoint, non-disjoint [3-5]. PHR-AODV builds compete or partial node-disjoint depend on topology. Figure 2 shows partial non-disjoint case.

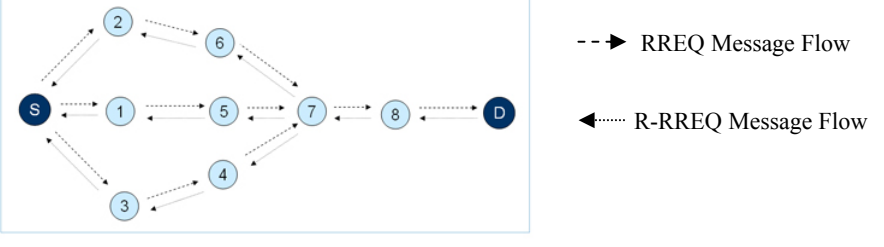

Fig. 2. Example of partial non-disjoint

Complete node-disjoint multipath is good for security, but partial node-disjoint multipath is also effective for security. We provide analytic method to estimate security. Let's assume some parameters: N_p is he number of nodes in routing path, N_{all} is the number of all nodes in network, M is the number of malicious nodes, (we assume that only one malicious node exists in the network), S is the number of paths from a source to a destination, ρ_m is probability of active malicious nodes.

$$\rho_m = \left(N_p \bullet M\right) / N_{all}. \tag{1}$$

We can calculate ρ_i, malicious node intrusion rate, as follows

$$\rho_i = \rho_m / S . \tag{2}$$

From formula 2, we obtain figure 3. The figure shows that increasing the number of paths derives decreasing of intrusion rate by a malicious node.

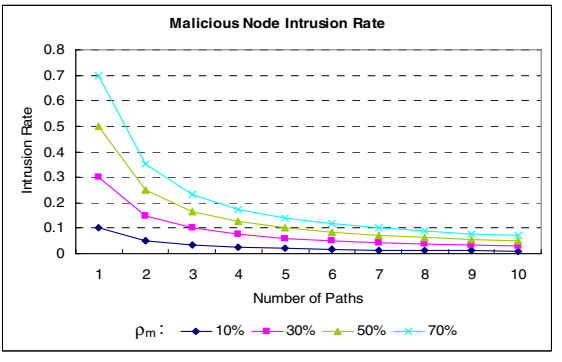

Fig. 3. Intrusion rate by a malicious node

3 Performance Results

We describe the simulation environment used in our study and then discuss the results in detail. Our simulations are implemented in Network Simulator (NS-2) [6].

We compare performance of AODV, R-AODV and PHR-AODV. Figure 4 shows packet deliver ratio of each protocol. R-AODV has better delivery ratio than other protocols have. PHR-AODV delivery ratio is less than other protocols, because it maintains more paths than others. Figure 5 shows the control packet overhead for setting routing paths. PHR-AODV has less packet overhead than that of R-AODV.

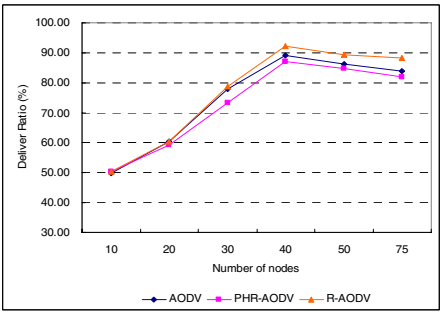

Fig. 4. Packet Delivery Ratio, when the number of nodes varies

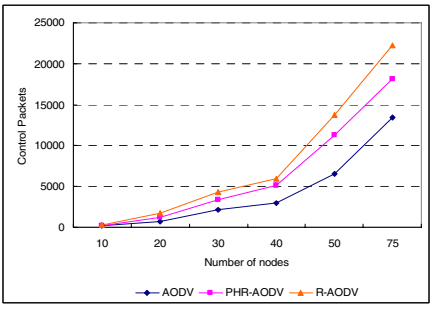

Fig. 5. Control Packet Overhead, when number of nodes varies

Figure 6 shows the average remained energy of each protocol. Figure 7 shows energy difference to express the distribution rate. PHR-AODV has less energy difference and balanced energy than others.

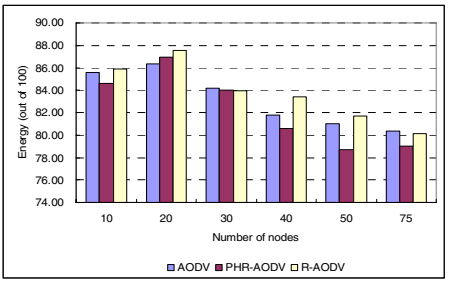

Fig. 6. Average energy remained, when number of nodes varies

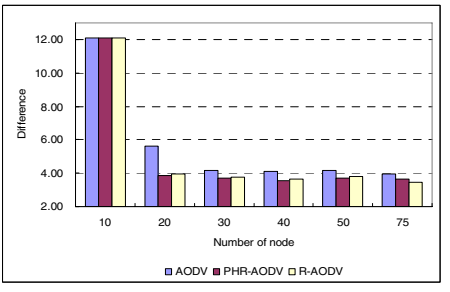

Fig. 7. Energy Difference, when number of nodes varies

4 Conclusions

Security is a significant issue in ad hoc networks. Intrusion of malicious nodes may cause serious impairment to the security. To decrease effect of malicious nodes, we proposed the idea of path hopping based on reverse AODV, in which the source node attempts to hop among available paths and split data. We conducted extensive analytic model and a simulation study to evaluate the performance of PHR-AODV with the R-AODV and AODV using NS-2. The results show that PHR-AODV maintains reasonable packet delivery ratio, energy consumption and energy distribution while increasing security of network. Our future work will focus on studying practical design and implementation for PHR-AODV.

References

1. C. Perkins, E. Belding-Royer Ad hoc on-Demand Distance Vector (AODV) Routing, RFC 3561, July 2003
2. Chonggun Kim, Elmurod Talipov, and Byoungchul Ahn, "A Reverse AODV Routing Protocol in Ad Hoc Mobile Networks" , LNCS 4097, pp. 522 – 531, 2006.
3. C. K.-L. Lee, X.-H. Lin, and Y.-K. Kwok, "A Multipath Ad Hoc Routing Approach to Combat Wireless Link Insecurity," Proc. ICC 2003, vol. 1, pp. 448–452, May 2003.
4. S.-J. Lee and M. Gerla, "Split Multipath Routing with Maximally Disjoint Paths in Ad Hoc Networks," Proc. ICC 2001, vol. 10, pp. 3201–3205, June 2001.
5. M. K. Marina and S. R. Das "On-Demand Multi Path Distance Vector Routing in Ad Hoc Networks," Proc. ICNP 2001, pp. 14– 23, Nov. 2001.
6. NS, The UCB/LBNL/VINT Network Simulator (NS), http://www.isi.edu/nsnam/ns/, 2004.
7. Zhi Li and Yu-Kwong Kwok, "A New Multipath Routing Approach to Enhancing TCP Security in Ad Hoc Wireless Networks" in Proc. ICPPW 2005.