International Journal of Information Processing, 8(2), 81-89, 2014
ISSN : 0973-8215
IK International Publishing House Pvt. Ltd., New Delhi, India

Blackhole Attack Defending Trusted On-Demand Routing in Wireless Ad-Hoc Network

Swarnali Hazra[a], S K Setua[a]

[a]Computer Science and Engineering, University of Calcutta, Kolkata, India,
Contact: swarnali.hazra@gmail.com, sksetua@gmail.com

Ad-hoc networks are vulnerable to blackhole attack. Blackhole attacker drops every incoming legitimate packet to exploit on-demand routing as well as data delivery in ad-hoc network. Blackhole attacker exploits on-demand routing by dropping route request packets. It drops route request packet instead of forwarding it and send route reply as if it has a valid route to destination. As a result, all data from source will be delivered towards blackhole attacker. In this paper, we have proposed a trusted approach to on-demand routing to defend blackhole attacker depending on our trust model with different level of trust computation. In our approach, Blackhole attackers are identified and isolated on the context of data forwarding. Analysis and simulation results justifies our proposal against blackhole attack for AODV, on-demand routing protocolin the form of Context Aware Trusted AODV Against Blackhole attack.

Keywords : AODV, Blackhole Attack, Direct Trust, Indirect Trust, Trustee, Trustor.

1. INTRODUCTION

On-demand routing protocols in ad-hoc network are not able to strongly defend blackhole attacker. When source needs to communicate with its target destination, source begin the discovery process for requisite route by broadcasting Route REQuest packet (RREQ) which floods the network until destination is found. When destination or an intermediate node that has a valid route to destination receives RREQ, it sends back a Route REply Packet (RREP) towards source. Source receives several RREPs which reached the source after traversing through different routes from the destination. Among all RREPs, source select the path which is traversed by the RREP of highest sequence number and of shortest hopcount for the communication. Blackhole attacker [1] exploits on-demand routing by dropping all received legitimate packets. Blackhole attacker drops the received RREQ and sends back false RREP with much higher sequence number towards source as if it has a valid route to destination, so that source select blackhole traversed highest sequence numbered path to communicate destination. After selecting data delivery route including blackhole attacker, when source try to send s necessary data to destination via blackhole attacker, blackhole attacker drops all data to disrupt the data delivery. We have considered the widely used AODV protocol [2] for on-demand routing.

Several existing proposals to protect AODV protocol against blackhole attack are based on threshold destination sequence number or RREP sequence number. In those proposals, source considers RREP as blackhole forwarded RREP if corresponding sequence number is higher than a threshold value. Again, if the sequence number of false RREP that forwarded by blackhole is not higher than threshold value and is of highest sequence number within the threshold value with shortest hop count, source selects the blackhole forwarded false RREP for data delivery path. In some proposals, source relies on acknowledgement of data receiving event by destination and in some other proposals, a RREP sending node is evaluated by the checking of data delivery rate. In such cases, blackhole attacker initially imple-

ther considered in the route dicovery process as case of belief, or discarded from route discovery as the case of disbelieve. As a result data delivery is done in secure manner. More research is needed to protect route discovery from several kinds of attacks. For further research, we will improve our proposed TOR model against other attacks in ad-hoc network.

REFERENCES

1. A Menaka and Pushpa M E. Effect of Black Hole Attack On AODV Routing Protocol in MANET, in *IJCST*, 4347(2), December 2010.
2. Stefano Basagni, Marko Conti, Silvia Giordano and Ivan Stojmenovic. Mobile Ad Hoc Networking (chapter: 10), *in A John Wiley and Sons, Inc., Publication*, 1999.
3. Mohammad Abu Obaida, Shahnewaz Ahmed Faisal, Md. Abu Horaira, Tanay Kumar Roy . (AODVR): An Analytic Approach to Shield Ad-hoc Networks from Black Holes, *in International Journal of Advanced Computer Science and Applications*, 2(8), December 2011.
4. Payal N Raj and Prashant B Swadas. DPRAODV: A Dynamic Learning System Against Blackhole Attack in AODV Based MANET, *in IJCSI*, 2, 2009.
5. Mehdi Medadian, Ahmad Mebadi and Elham Shahri. Combat with Black Hole Attack in AODV Routing Protocol, *in IEEE*, 2009.
6. L Capra. Toward a Human Trust Model for Mobile Ad-hoc Networks, *Proceedings of* 2^{nd} *UK-UbiNet Workshop*, Cambridge University, Cambridge, UK, May 2004.
7. H Li and M Singhal. Trust Management in Distributed Systems, *Computers*, 40(2):45–53, 2007.
8. E Aivaloglou, S Gritxalis and C Skianis. Trust Establishment in Ad Hoc and Sensor Networks, *International Workshop on Critical Information Infrastructure Security, Lecture Notes in Computer Science, Spinger*, 4347:179–192, 2006.
9. J S Baras and T Jiang. Managing Trust in Self-Organized Mobile Ad Hoc Networks, *in* 12^{th} *Annual Network and Distributed System Security Symposium Workshop*, 2005.
10. Latha Tamilselvan and V Sankaranarayanan. Prevention of Co-operative Black Hole Attack in MANET, *in Journal of Networks*, 3(5), May 2008.

Swarnali Hazra received her B.Tech from West Bengal University of Technology, M.Tech from University of Calcutta Computer Science and Engineering. Currently she is Ph.D scholar of University of Calcutta. Her research interests include Ad-hoc Network, Network Security, Sensor Network, Routing, Clustering, Graph Theory *etc.*. She has published many research papers in international journals and conferences.

S K Setua received his B.Tech and M.Tech from University of Calcutta Computer Science and Engineering. He is currently Associate Professor in the University of Calcutta. His research interests include Network Security, Sensor Network, Ad-hoc Network, Routing, Clustering, Image Processing, Graph Theory, Distributed Computing, Cloud Computing, Database Security, DNA Computing, Big Data, Cliford Algebra *etc.*. He has published many research papers in international journals and conferences.