A Secure Routing Protocol to Prevent Cooperative Black Hole Attack in MANET

Nai-Wei Lo and Fang-Ling Liu

Abstract As a mobile ad hoc network (MANET) is dynamically formed by wireless mobile devices, which generally have limited computing resources, low network bandwidth accessibility, and limited power supply, and does not have any physical infrastructure and central base station, network management and operations are done cooperatively by all mobile devices in the network. In consequence, malicious mobile devices can easily join a MANET and launch attacks. Among those attacks, cooperative black hole attack requiring at least two malicious device nodes is a serious security threat since this attack is very easy to launch and hard to detect by other nodes. In this study, we introduce a secure routing protocol to defend against the cooperative black hole attack. Simulation experiments using QualNet has shown that our protocol provides up to 2.6 times performance in terms of the packet delivery ratio when comparing with AODV protocol under cooperative black hole attack.

Keywords Mobile ad hoc network • Cooperative black hole attack • Secure routing protocol

1 Introduction

Mobile ad hoc network (MANET) is dynamically formed by a set of mobile devices through their wireless communication capability. Therefore, MANET does not have physical infrastructure and central base station. Network topology will change any time due to dynamic movement of mobile devices and the wireless signal roaming range of each mobile device. Network management is dependent on the

N.-W. Lo (✉) • F.-L. Liu
Department of Information Management, National Taiwan University of Science and Technology, Taipei 106, Taiwan
e-mail: nwlo@cs.ntust.edu.tw

J. Juang and Y.-C. Huang (eds.), *Intelligent Technologies and Engineering Systems*, Lecture Notes in Electrical Engineering 234, DOI 10.1007/978-1-4614-6747-2_8,

cooperation among mobile nodes. In addition, the average life time of MANET is relatively short in comparison with wired network because mobile devices equip limited computing resources and battery power in general.

With increasing deployment and usage on military operations, enterprise meeting rooms, home networking, and vehicular traffic management systems, MANET security has become an important issue. Since network management and operations in MANET are dependent on cooperation of all mobile nodes, it is very easy for a MANET to encounter security threats and various attacks [1]. Malicious mobile devices can easily join a MANET and launch attacks. Among those attacks, cooperative black hole attack is a serious security threat since this attack is very easy to launch and hard to detect by other nodes [2]. To launch a cooperative black hole attack requires at least two malicious device nodes existing in the same MANET.

Since mobile devices have limited power supply, routing protocols used for MANET have to reduce energy consumption while establishing and maintaining packet (message) routes. From previous literature [3], it is shown that proactive protocols such as optimized link state routing protocol (OLSR) consume more energy than reactive protocols such as ad hoc on-demand distance vector protocol (AODV) [4] and dynamic source routing protocol (DSR) in general. In addition, regarding the two most dominant reactive routing protocols, AODV and DSR, AODV is more efficient and effective in comparison with DSR in general MANET environments [5]. Therefore, our study on cooperative black hole attack assumes AODV protocol is utilized in MANET.

Black hole attack is the simple version of cooperative black hole attack. When there is only one malicious node in MANET, this adversary can launch black hole attack by forging and replying the shortest packet transmission path, which will route through the malicious node itself, to the source node which is sending RREQ routing request control packets to establish a route for its destination. Once the source node selects the forged route and starts to use it as the delivering route for its data packets, the malicious node will deliberately drop all received data packets from the source node. In consequence, all data packets transmitted from the source node are vanished or absorbed by "a black hole" (the malicious node) and the destination node will never receive any data packet through the forged route. To defend against black hole attack, various mechanisms and protocols have been developed based on AODV [6–9]. In [6], three rules are set in each source node to assess plausibility of replied routes and select the target route. In [7], MOSAODV mechanism is proposed. Within MOSAODV, each source node will set a timer to collect all replied RREP packets and then discard those RREP packets with exceptionally high destination sequence numbers. In addition, the names of all identified malicious nodes will be stored in a blacklist table in each node. In [8], SAODV mechanism is introduced. Within SAODV, a source node collects routing information of its neighbors to determine which replied route it should select. Basically, the source node will select one of the replied routes in which all routes contain the same routing node as next hop, and the total number of these routes is the largest one compared to other possible routes. In [9], DPRAODV mechanism is introduced. In DPRAODV scheme, a threshold of valid RREP sequence number

is dynamically derived to evaluate the sequence numbers of received RREP packets for each wireless communication request process.

The attack model of cooperative black hole attack is the same as black hole attack. However, at least two malicious nodes are required to work together and launch a cooperative black hole attack. The two (or more) malicious nodes need to establish direct wireless communication link (hop) in advance. We refer the malicious node which is near the source node in terms of wireless connection path as the first malicious node. The other malicious node indicates as the second malicious node. The first malicious node tries to establish wireless communication route with the source node during the first step of cooperative black hole attack. Once the communication route passing through the first and second malicious nodes between the source node and the destination node is established, data packets will send through this route and reach the first malicious node. Then the first malicious node will forward the received data packets to the second malicious node along with their direct connected wireless link. Finally, the second malicious node drops the received data packets and successfully fulfills the cooperative black hole attack. As the first malicious node establishes data transmission route and the second malicious node drops transmitted data packets, it is more difficult to defend against cooperative black hole attack.

Several solutions have been proposed to defend against cooperative black hole attack in recent years [10–12]. In [10], Ramaswamy et al. proposed a solution to defend against cooperative black hole attack. A table containing data routing information (DRI) and a corresponding cross-checking method are installed at each mobile node. Each node observes its neighboring nodes and records whether its neighbors transmitting data packets to next corresponding nodes. All observed results are recorded in the DRI table, and each node determines which neighbors are not reliable based on its DRI table. Weerasinghe and Fu in [11] proposed an enhanced solution to identify and isolate nodes that invoke cooperative black hole attack using mechanisms proposed in [10] plus the usage of two new control packets: further request (FREQ) and further reply (FREP). In [12], Tamilselvan and Sankaranarayanan introduced a new concept called fidelity level to indicate the reliability of an observing node. A detection mechanism for cooperative black hole attack is developed by introducing a fidelity table into each node. An observing node with its fidelity level value 0 is considered as a malicious node, and all possible routing paths through this node will be eliminated by the observer (a mobile node). As the detection mechanism in [12] is derived based on AODV routing protocol, this mechanism will select a candidate route through a neighbor node with higher fidelity level for the observer if two RREP packets from different routing paths are received by the observer at the same time. In addition, the observer will broadcast the names of identified malicious nodes through ALARM control packets to other nodes in MANET.

In this study, we observed that previously proposed solutions require a lot of communications among nodes in MANET to observe neighboring nodes, identify malicious nodes, and broadcast the blacklist of detected malicious nodes. In consequence, control overhead can be very heavy. In addition, malicious nodes

may intentionally broadcast false blacklist to all nodes in MANET and easily paralyze the entire network. Therefore, we propose a new mechanism to resolve cooperative black hole attack without using blacklist or constant message (control packet) exchange.

2 The Proposed Detection Mechanism

For simplicity on detection mechanism description, we depict our detection methodology based on AODV routing protocol. The proposed detection mechanism is abbreviated as CBDAODV to indicate the full name of cooperative black hole attack detection mechanism based on AODV. We also define our attack model as follows. To form a cooperative black hole attack group, at least two malicious nodes can communicate to each other through one hop distance. For an attack group with two malicious nodes, either both nodes drop data packets or only the last (second) node drops data packets. Every node has its own blacklist but not broadcasts its blacklist to other nodes.

In a cooperative black hole attack, the first malicious node in the attack group will send out RREP control packets back to the source node who broadcasted RREQ connection requests. To increase the possibility that the RREP sent by the first malicious node is the earliest one to arrive at the source node, the best location for the first adversary is to become a neighboring node of the source node. In general, the false routing path replied by the first malicious node will pass through the first adversary and then reach to the second malicious node. Moreover, the second adversary does not actually have routes connecting to the destination node. Based on this observation, the concept of CBDAODV is developed. In CBDAODV, a source node will accept at least two RREP packets from different replying nodes; therefore, the source node knows two routes to reach the destination. By utilizing another routing path to verify the reliability of selected routing path, the source node itself can evaluate the currently selected routing path and make rerouting decision once it suspects the reliability of currently selected route. A confirmation control packet is invented by CBDAODV for the source node to send through another route, presumably a slower one than the selected one, to the destination node. The confirmation packet contains the name of the second malicious node which is observed and recorded by the source node when the first malicious node sends corresponding data packets to the second malicious node. Once receiving the confirmation packet, the destination node will reply it to indicate whether there exists a route between the destination node and the second malicious node. If the confirmation reply packet indicates there is no route between the destination node and the second malicious node, then the source node will know the second malicious node is a malicious node and it is executing a black hole attack. The source node now switches its routing path to another one and retransmits its data packets. At the same time, the source node will put the first malicious node into observation; if this malicious node regularly uses the second malicious node as its

next hop destination for all upcoming routing paths requested by the source node, then the source node can identify the first malicious node is belonging to the cooperative black hole attack group.

3 Simulation Results and Analysis

To evaluate the proposed CBDAODV mechanism, a set of simulation experiments are conducted by developing CBDAODV algorithm on QualNet 5.0 simulator. The simulated terrain area for a MANET is 800 m × 800 m, and there are 25 mobile nodes dynamically moving around for 600 s of simulation time. Two out of 25 nodes are defined as malicious nodes when necessary. The random waypoint model is used to model node mobility. The moving speed of each node is between 10 and 60 m/s. Packets transmitted among nodes are generated in constant bit rate (CBR). For each node, the pause time for change of moving speed and direction is 10 s. The wireless transmission range for a node is defined as 250 m. The size of data packet is 512 bytes. Regular AODV protocol without encountering cooperative black hole attack (AODV), AODV protocol with the occurrence of cooperative black hole attack (blackholeAODV), and AODV protocol implemented with our detection mechanism (CBDAODV) are compared in terms of packet delivery ratio and average end-to-end delay. From Fig. 1, when AODV is under cooperative black hole attack, the packet delivery ratio only has 20–40 %. With CBDAODV installed, the packet delivery ratio maintains at 70–80 % while suffering from the attack. That is, the CBDAODV mechanism effectively defends against cooperative black hole attack and provides up to 2.6 times packet delivery ratio in comparison with AODV without implementing any defense mechanism. In Fig. 2, CBDAODV has a slightly higher average end-to-end delay than regular

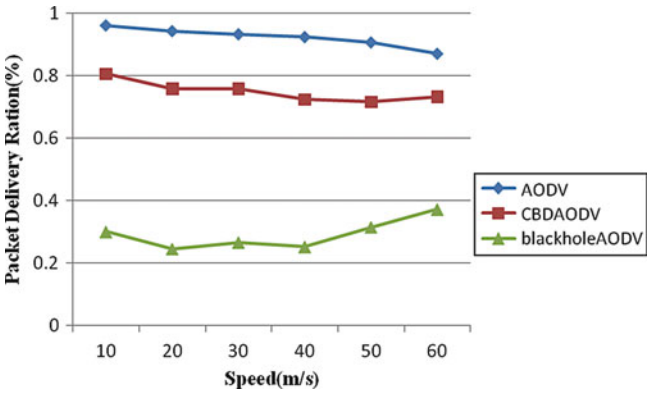

Fig. 1 Comparison on packet delivery ratio among three protocol conditions

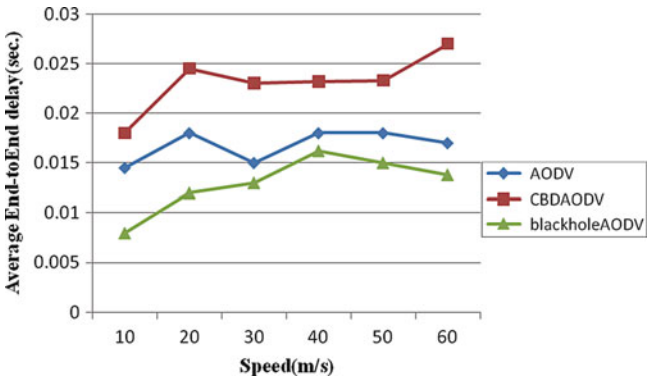

Fig. 2 Comparison on average end-to-end delay among three protocol conditions

AODV and AODV under the attack. This is because the nodes with CBDAODV wait for the second arriving RREP packet from different nodes to get the second routing path before sending data packets through the first selected routing path.

4 Conclusion

In this study, an effective detection mechanism for cooperative black hole attack is developed. This mechanism provides up to 2.6 times performance in terms of the packet delivery ratio when comparing with AODV protocol under cooperative black hole attack. In addition, no alarm packets broadcast or blacklist broadcast is required in our solution when malicious nodes were identified.

Acknowledgments The authors gratefully acknowledge the support from Taiwan Information Security Center (TWISC) and National Science Council, Taiwan, under the grant numbers NSC 101-2219-E-011-004 and NSC 101-2218-E-011-004.

References

1. Deng H, Li W, Agrawal DP (2002) Routing security in wireless ad hoc networks. IEEE Commun Mag 40(10):70–75
2. Abusalah L, Khokhar A, Guizani M (2008) A survey of secure mobile ad hoc routing protocols. IEEE Commun Surv Tutor 10(4):78–93
3. Mbarushimana C, Shahrabi A (2007) Comparative study of reactive and proactive routing protocols performance in mobile ad hoc networks. In: 21st international conference on advanced information networking and applications workshops/symposia, IEEE Press, New York, pp 679–684
4. Perkins CE, Belding-Royer E, Das S (2003) Ad hoc on-demand distance vector (AODV) routing. The Internet Engineering Task Force (IETF) RFC 3561

5. Khatri P, Rajput M, Shastri A, Solanki K (2010) Performance study of ad-hoc reactive routing protocols. J Comput Sci 6(10):1159–1163
6. Medadian M, Yektaie MH, Rahmani AM (2009) Combat with black hole attack in AODV routing protocol in MANET. In: First asian himalayas international conference on internet, IEEE Press, New York, pp 1–5
7. Mistry NH, Jinwala DC, Zaveri MA (2009) MOSAODV: solution to secure AODV against blackhole attack. Int J Comput Netw Secur 1(3):42–45
8. Tamilselvan L, Sankaranarayanan V (2007) Prevention of blackhole attack in MANET. In: The 2nd international conference on wireless broadband and ultra wideband communications, IEEE Press, New York, pp 21–26
9. Raj PN, Swadas PB (2009) DPRAODV: a dynamic learning system against blackhole attack in AODV based MANET. IJCSI Int J Comput Sci Issues 2:54–59
10. Ramaswamy S, Fu H, Sreekantaradhya M, Dixon J, Nygard K (2003) Prevention of cooperative black hole attack in wireless ad hoc networks. In: The 2003 international conference on wireless networks, CSREA Press, Las Vegas, pp 570–575
11. Weerasinghe H, Fu H (2007) Preventing cooperative black hole attacks in mobile Ad Hoc networks: simulation implementation and evaluation. In: Future generation communication and networking. IEEE Press, New York, pp 362–367
12. Tamilselvan L, Sankaranarayanan V (2008) Prevention of cooperative black hole attack in MANET. J Netw 3(5):13–20