The Impact of Resource Consumption Attack on Mobile Ad-hoc Network Routing

Maha Abdelhaq[1], Raed Alsaqour[1], Mohammed Al-Hubaishi[2,3], Tariq Alahdal[2], and Mueen Uddin[4,5]
(Corresponding Author: Maha Abdelhaq)

School of Computer Science, Faculty of Information Science and Technology,University Kebangsaan Malaysia[1]
43600,UKM, Bangi, Selangor Darul Ehsan, Malaysia
Faculty of Computer Science & Information System, Thamar University, Thamar, Republic of Yemen[2]
LAB, FCT-DEEI, Universidade Algarve Portugal, Faro, Portugal[3]
Kulliah of Information and Communication Technology, International Islamic University Malaysia[4]
Asia Pacific University of Technology and Innovation, Kuala Lumpur, Malaysia[5]
(Email: maha.ukm@gmail.com)

(Received Feb. 3, 2013; revised and accepted July 12, 2013)

Abstract

Mobile Ad Hoc Network (MANET) is a temporary network of mobile nodes where mobile nodes communicate with each other through wireless links with no fixed infrastructure and no centralized control. Each mobile node in such a scenario acts as both a router and host. Security is an important issue in the MANET environment because of its dynamic topology and limited range of each mobile host's wireless transmissions. This paper introduces a simulation-based study for the impact of Resource Consumption Attack (RCA) on MANET performance. RCA is one of the Denial of Service attacks (DoS) in which the attacker keeps broadcasting Route Request (RREQ) packets in order to degrade the network overall performance. Specifically, this paper examined how differing the number of attackers and their positions could affect MANET packet delivery ratio and delay jitter. The paper results open the door for suggesting an intrusion detection system in order to mitigate and prevent RCA terrible effects on MANET.

Keywords: *Denial of service attack, mobile ad-hoc network, resource consumption attack, security*

1 Introduction

MANET has been a challenging research area for the last few years because of its dynamic topology, power constraints and limited range of each mobile host's wireless transmissions and security issues.

MANET is a rapidly deployable, self-organized and multi-hop wireless network. It is typically set up for limited periods of time and particular applications such as military, disaster areas and medical applications. Nodes in MANET may move arbitrarily while communicating over wireless links. This network is typically used in situations where there is no centralized administration or support from networking infrastructure such as routers or base stations.

Many up-to-date researches pay attention to MANET as a new technology with specific characteristics which distinguish it from other types of networks, such as openness which simplifies the way for external attacks to join the trusted nodes easily, resource limitation in power and bandwidth, mobility and dynamicity, flexibility, distributed computation and decentralizatio [6, 22].

It is apparent that these characteristics render MANET environment susceptible to different types of attacks. However, the attacking effects on the targeted nodes differ according to specific attacking scenarios and factors such as the number of attacks and their positions. Hence, it is of interest to see how a specific type of attack is performed over particular routing protocol in order to protect MANET from its violation. Therefore, this paper introduces a detailed analysis for RCA scenarios over Ad-hoc on Demand Distance Vector (AODV) routing protocol and the impacts of each scenario on MANET's functionality represented by packet delivery ratio and delay jitter performance metrics.

This paper is structured as follows: Section 2 introduces a literature review for the previous works. Section 3 presents AODV routing protocol. Then, Section 4 explains the AODV vulnerability to RCA. After that, Section 5 highlights the simulation environment. Section 6 presents the simulation results and finally Section 7 presents the research conclusion and future work.

2 Related Work

Ning and Sun in [14], introduced a systematic analysis of the impact of two main categories of attacks over AODV: atomic misuse in which the attacker misuses only one routing packet, and compound misuse which comprises several types of atomic misuses attacks. They defined

several attack actions and how each action could be performed over each routing packet in AODV routing protocol. Also, they defined the goals of each attack manipulation. Their study is useful for researchers who are interested in developing intrusion detection systems such as the one proposed in [2]. However, the study did not include one of the most dangerous attacks over AODV which is RCA.

Gu *et al.* In [7] introduced a deep study of one type of Distributed Denial of Service (DDoS) attacks namely flooding attack [8, 9, 19, 20]. Specifically, they analyzed the effect of both the remote flooding attack and the local flooding attack on the throughput performance metric of MANET [11, 12].

Karlof and Wagner in [9] performed a detailed analysis of various attacks against both sensor networks and MANET. Their analysis includes Hello floods, sinkhole, acknowledge spoofing, wormhole, selective forwarding and Sybil attacks.

Marti *et al*. In [11] explained how dropping packets attack could be performed over MANET. Kurosawa *et al.* in [10] studied an interpretation for the effects of the black hole attack on the AODV routing protocol over MANET [1]. On the other hand, Padilla *et al.* [6] analyzed how the black hole attack could paralyze the functionality of the Optimized Link State Routing protocol (OLSR). Their work focused on OLSR over a particular type of MANET environment termed as Tactical MANET.

Wallenta *et al.* In [21] studied the impact of cache poisoning attack over wireless sensor networks through different parameters. To the best of our knowledge, no research has investigated the impact of RCA on the performance of AODV according to both packet delivery ratio and delay jitter by varying the number of attackers and their attack positions.

3 Ad Hoc On-Demand Distance Vector Routing Protocol

This research work uses the AODV routing protocol [15, 16, 18]. AODV is a reactive self-starting and large scale routing protocol. It has been extensively studied and developed over many years, which proves its robustness and benefits.

The main advantages of the AODV protocol are: firstly, the connection setup delay with the destination is lower compared with other MANET routing protocols. Secondly, AODV avoids the congested paths in comparison with the other ad hoc routing protocols. Thirdly, it can cope with the rapid ad hoc topological reconfigurations that may affect the other routing protocols [18]. However, AODV is vulnerable to different types of attacks. The following subsections explain how AODV is vulnerable to RCA over MANET.

In the route discovery process of the AODV routing protocol over MANET, source node broadcasts a route request (RREQ) packet throughout MANET nodes - as shown in Figure 1 - and sets a timer waiting for the reply. The RREQ packet contains routing information such as: the originator IP address, the broadcast ID, and the destination sequence number.

Each intermediate node receives the RREQ packet and keeps the reverse path to the source node besides performing two processes: firstly, it verifies if it has received the RREQ packet before with the same originator IP address and broadcast ID, then decides either to discard the RREQ packet or accept it. This verification process helps prevent flooding attacks. Secondly, if the RREQ packet is accepted, the intermediate node checks the destination sequence number stored in its routing table. If it is greater than or equal to the one stored in the RREQ packet it uni-casts the route reply (RREP) packet to the source node. If no intermediate node has a fresh enough (fresh destination sequence number) route to the destination node, the RREQ packet keeps its navigation until it reaches the destination node itself which in turn unicasts the RREP packet towards the source node as shown in Figure 2.

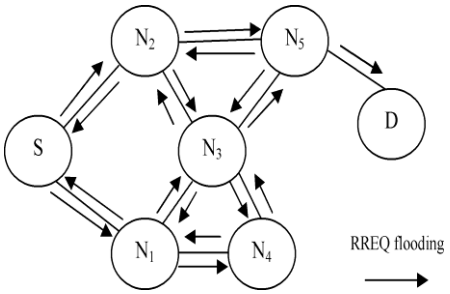

Figure 1: Propagation of RREQ packet; S: source node, D: destination node, N_1 to N_5 intermediate nodes

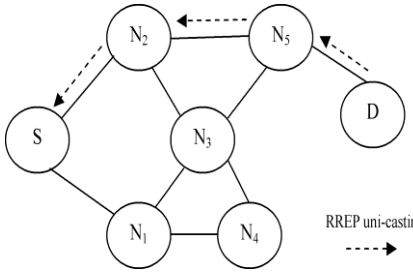

Figure 2: The path of RREP packet; S: source node, D: destination node, N_1 to N_5 intermediate nodes

4 The Vulnerability of AODV to RCA

RCA [3, 4, 13, 22] is one of the DoS attacks in which the attacker exploits the route discovery process in the AODV routing protocol. The attacker, as shown in Figure 3, keeps broadcasting the RREQ packet with a different broadcast ID in order to notify each node broadcasting continuously and consume its limited resource of energy, bandwidth, and memory.

As noticed, the attacker does not follow AODV rules. Therefore, to achieve its attack successfully, it does not set a timer waiting for a reply but keeps overflowing the network with RREQ packets as shown in Figure 4. In

Figure 4, if destination node D represents a server, then its service could be isolated by the attacker A.

of the link extremely easily and quickly. When MANET links have been over flown with malicious packets, the congested links would be jammed which leads to interrupted accessing services of the available servers in the network.

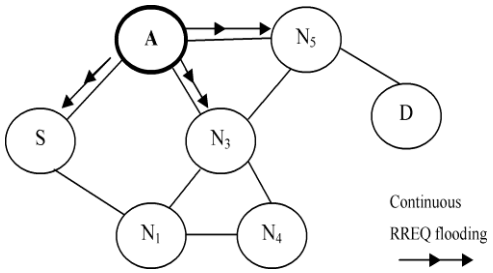

Figure 3: RREQ continuously broadcasted by RCA; S: source node, D: destination node, A: attacker

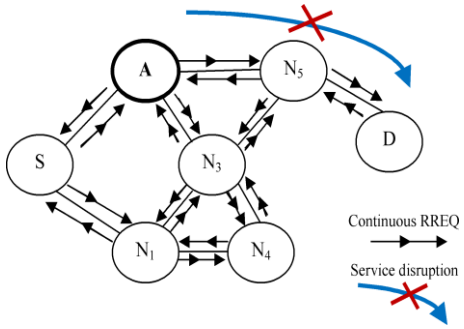

Figure 4: RREQ packets flooded by RCA; S: source node, D: destination node, A: attacker

5 Simulation Enviroment

This section explains the environment where our experimental simulations are performed. Specifically, the simulation parameters and main performance metrics used are discussed.

The simulation experiments were carried out using Qualnet 5.0.2 [17]. Table 1 shows the main fixed parameters considered in each experiment scenario. The preliminary goal of the experiments' scenarios is to assess the impact of RCA on the network performance by varying the number of attackers and their attack positions. Therefore, the number of attackers varies in the experiments' scenarios from zero to ten attackers. Also, each certain number of attackers has been tested in three attack positions which are: near sender, near receiver, and random. In near sender scenario (Figure 5a), the attackers flood the RREQ packets towards the source node even through one hop (if the attacker is a neighbor to the source node) or more using the other legitimate nodes. However, in near receiver scenario (Figure 5b), the attackers flood the RREQ packets towards the destination node in the same way as aforementioned. On the other hand, in random positions scenario (Figure 5c), the attackers are located in a random fashion that enables them to target the source node, the destination node and the path between each of them.

MANET is extremely vulnerable to this type of attack since its limited bandwidth capacity simplifies overflowing

The performance metrics used are:

1. Packet delivery ratio: Packet delivery ratio is the ratio of the number of data packets successfully delivered to the destination to those generated by CBR source.
2. Delay jitter: Delay jitter is the variation in the time between packets arriving at the destination, caused by network congestion, timing drift, or route changes.

In our experiments' results, each scenario result represents the average of five simulation runs.

Table 1: Simulation parameters

Parameter	Value
Simulation time	200 s
Number of nodes	100 without attackers
Attack rate	10 RREQ/s
Mobility model	Random way point
Min-max speed	0-8 m/s
Radio type	802.11b
Antenna model	Omnidirectional
Terrain dimensions	1500x1500
Pathloss model	Two-ray
Transmission range	250m
Packet size	512 bytes
Mobility model	Random way point
Traffic model	CBR

6 Results and Discussion

Figure 6 and 7 depicts that the average results of the attackers' placements show that near receiver placement scenario outperforms the others in degrading the packet delivery ratio in the network. This is because packet delivery ratio means the ratio of the number of packets received by the receiver to the number of the packets actually sent by the sender. Therefore, when attackers are located near receiver, they reduce the possibility of receiving the already produced and sent packets which leads to an overall packet delivery ratio degradation.

Figure 8 ensures that the max effect on the delay jitter achieved by the attackers near sender when they are 8 attackers. In specific, near sender attackers could increase the delay jitter by 87.9% compared to the normal case, while near receiver and randomly located attackers could increase it by 84.5% and 84.9% in the max increase respectively. Also, Figure 9 depicts that near sender attackers have the strongest effect on the normal nodes' packets delay jitter if we consider the average effect of attackers which are varied from 2 to 10.

7 Conclusion and Future Work

In this paper, we studied the impact of RCA over AODV routing protocol in MANET. The study focused on assessing the effect of varying the number of attackers and their placements on two performance metrics which are

packet delivery ratio and delay jitter. The study opens the door to the researchers to suggest solutions which could mitigate the impact of RCA.

In the future, we aim to study the impact of RCA on other performance metrics such as: throughput, end-to-end delay, energy consumption and routing packets overhead. Also, the study could include more attacking scenarios such testing the effect of attackers' radio range and flooding rate. Our concern also to modify AODV protocol to have security protection against RCA.

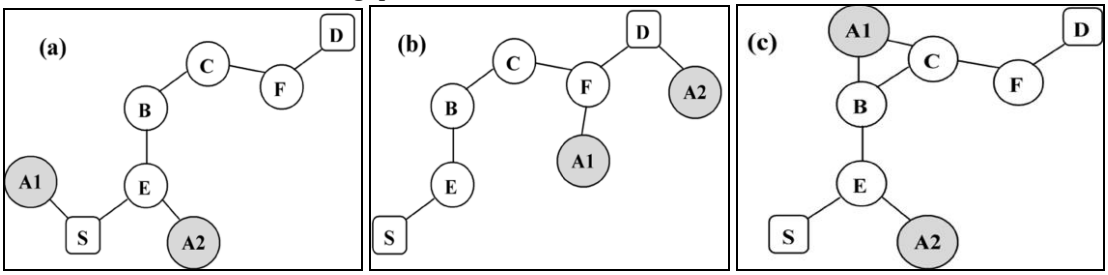

Figure 5: Distribution of RCA attackers with different positions. (a) Attackers A1 and A2 are one hop and two hops away from source S, respectively. (b) Attackers A1 and A2 are two hops and one hop away from destination D, respectively. (c) AttackersA1 and A2 are randomly located along the path between source S and destination D.

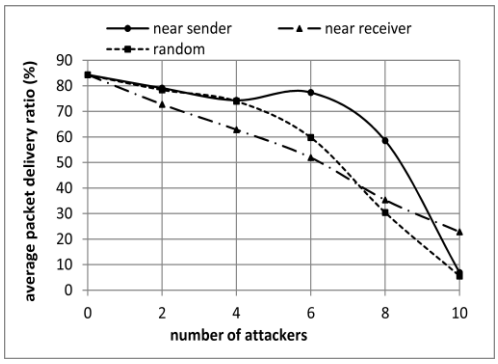

Figure 6: Packet delivery ratio vs number of RCA attackers

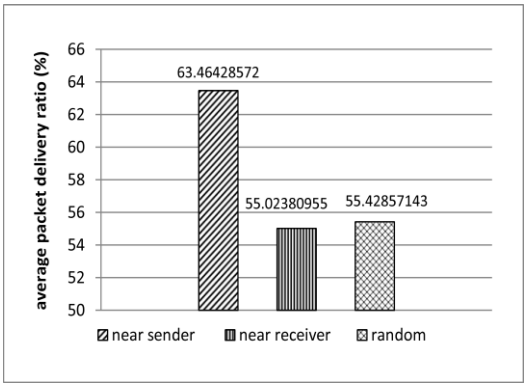

Figure 7: Packet delivery ratio vs RCA attackers' location

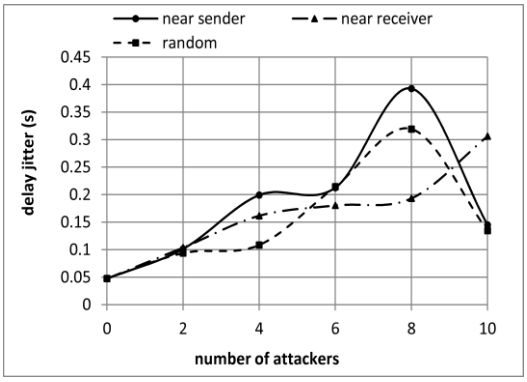

Figure 8: Delay jitter vs number of RCA attackers

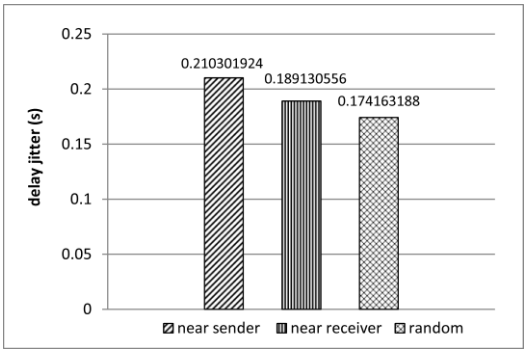

Figure 9: Delay jitter RCA attackers' location

References

[1] M. Abdelhaq, S. Serhan, R. Alsaqour, and A. Satria, "Security routing mechanism for black hole attack over AODV MANET routing protocol," *Australian Journal of Basic and Applied Sciences*, vol. 5, pp. 1137-1145, 2011.

[2] M. Abdelhaq, S. Serhan, R. Alsaqour, and R. Hassan, "A local intrusion detection routing security over MANET network," in *International Conference on Electrical Engineering and Informatics*, pp. 1-6, 2011.

[3] M. Abdelhaq, R. Hassan, and R. Alsaqour, "Using dendritic cell algorithm to detect the resource consumption attack over MANET," in *Software Engineering and Computer Systems*, LNCS 181, pp. 429-442, Springer-Verlag, 2011.

[4] S. Agrawal, S. Jain, and S. Sharma, "A survey of routing attacks and security measures in mobile ad-hoc networks," *Arxiv preprint arXiv:1105.5623*, 2011.

[5] E. Cayirci and C. Rong, *Security in Wireless Ad Hoc and Sensor Networks*, Wiley Online Library, 2009.

[6] E. Gerhards-Padilla, N. Aschenbruck, P. Martini, M. Jahnke, and J. Tolle, "Detecting black hole attacks in tactical MANETs using topology graphs," in *The 32nd*

IEEE Conference on Local Computer Networks, pp. 1043-1052, 2007.

[7] Q. Gu, P. Liu and C. H. Chu, "Analysis of area-congestion-based DDoS attacks in ad hoc networks," *Ad Hoc Networks*, vol. 5, pp. 613-625, 2007.

[8] B. B. Gupta, R. C. Joshi, and M. Misra, "ANN based scheme to predict number of zombies in a DDoS attack," *International Journal of Network Security*, vol. 14, pp. 61-70, 2012.

[9] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures," *Ad Hoc Networks*, vol. 1, pp. 293-315, 2003.

[10] S. Kurosawa, H. Nakayama, N. Kato, A. Jamalipour, and Y. Nemoto, "Detecting blackhole attack on AODV-based mobile ad hoc networks by dynamic learning method," *International Journal of Network Security*, vol. 5, pp. 338-346, 2007.

[11] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in *International Conference on Mobile Computing and Networking*, pp. 255-265, 2000.

[12] R. Murugan and A. Shanmugam, "A timer based acknowledgement scheme for node misbehavior detection and isolation in MANET," *International Journal of Network Security*, vol. 15, pp. 241-247, 2013.

[13] A. Nadeem and M. Howarth, "Adaptive intrusion detection & prevention of denial of service attacks in MANETs," in *Proceedings of the 2009 International Conference on Wireless Communications and Mobile Computing: Connecting the World Wirelessly*, pp. 926-930, 2009.

[14] P. Ning and K. Sun, "How to misuse AODV: A case study of insider attacks against mobile ad-hoc routing protocols," *Ad Hoc Networks*, vol. 3, pp. 795-819, 2005.

[15] C. E. Perkins, E. Belding-Royer and S. Das, *Ad hoc On-Demand Distance Vector (AODV) Routing*, IETF MANET Internet Draft, 2003.

[16] C. E. Perkins and E. M. Royer, "Ad-hoc on-demand distance vector routing," in *Second IEEE Workshop on Mobile Computing Systems and Applications*, pp. 90-100, 1999.

[17] Q. N. Simulator, *Scalable Network Technologies*, Inc, 2011. (http://www.qualnet.com)

[18] S. Taneja and A. Kush, "A survey of routing protocols in mobile ad hoc networks," *International Journal of Innovation, Management and Technology*, vol. 1, pp. 279-285, 2010.

[19] M. Uddin, R. Alsaqour and M. Abdelhaq, "Intrusion detection system to detect DDoS attack in gnutella hybrid P2P network," *Indian Journal of Science and Technology*, vol. 6, pp. 4045-4057, 2013.

[20] J. Udhayan and T. Hamsapriya, "Statistical segregation method to minimize the false detections during DDoS attacks," I*nternational Journal of Network Security*, vol. 13, pp. 152-160, 2011.

[21] C. Wallenta, J. Kim, P. J. Bentley, and S. Hailes, "Detecting interest cache poisoning in sensor networks using an artificial immune algorithm," *Applied Intelligence*, vol. 32, pp. 1-26, 2010.

[22] D. Wang, M. Hu and, H. Zhi, "A survey of secure routing in ad hoc networks," in *The Ninth International Conference on Web-Age Information Management*, pp. 482-486, 2008.

Maha Abdelhaq received her Bachelor and Master degrees in Computer Science in 2006 and 2008 from Jordan University, (Amman, Jordan). She expected to receive her PhD degree in wireless ad hoc network security in August 2013 from Universiti Kebangsaan Malaysia, Malaysia. Her research interests include ad hoc network, routing protocols, network security, artificial computational intelligence and network performance evaluation.

Raed Alsaqour is an Assistant Professor in the Computer Science Department, Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia, Malaysia. He received his B.Sc. degree in computer science from Mu'tah University, Jordan, in 1997. M.Sc. degree in distributed system from University Putra Malaysia, Malaysia, in 2003 and his PhD degree in wireless communication system from Universiti Kebangsaan Malaysia, Malaysia, in 2008. His research interests include wireless network, ad hoc network, vehicular network, routing protocols, simulation, and network performance evaluation. He also has a keen interest in computational intelligence algorithms (fuzzy logic and genetic) applications and security issues (intrusion detection and prevention) over network.

Mohammed Al-Hubaishi is a Lecturer and Researcher in the Faculty of Computer Science and Information System, Thamar University, Yemen. He received his B.Sc. degree in computer science from Thamar University, Yemen, in 2002. In December 2010, he has M.Sc. degree in wireless ad hoc network from Department of Electronic and Informatics Engineering Faculty of University of Algarve, Portugal. His research interests include wireless network, ad hoc network, routing protocols, multimedia and NS2 simulation. He is also interested in Internet programming and website design using HTML, CSS, PHP and JavaScript languages.

Tariq Abdullah is an Assistant Professor in the Computer Science Department, Faculty of Computer Science and Information System, Thamar University, Yemen. He received his B.Sc. degree in computer science from Baghdad University, Iraq, in 1998 and his M.Sc. and PhD degrees in distributed system and wireless communication from University Putra Malaysia, Malaysia, in 2003 and 2008 respectively. His research interests include wireless network, ad hoc network, WiMAX core network, routing

protocols, simulation, and wireless communications. He also has a growing interest in multihop and network architecture for intelligent cloud base station.

Mueen Uddin is a Senior Lecturer at Faculty of Computing and Technology, Asia Pacific University of Technology & Innovation. He completed his PhD in Information Systems from UTM Malaysia in 2012, BS & MS in Computer Science from Isra University Hyderabad Pakistan in 2008 with specialty in Information networks. His research interests include Green IT, energy efficient data centers and Virtualization technologies, digital content protection and deep packet inspection, intrusion detection and prevention systems, MANET routing protocols and their analysis. Dr. Mueen has over 22 international Journal publications and many Conference papers.