A Study on the Vulnerability of AODV Routing Protocol to Resource Consumption Attack

Maha Abdelhaq[1], Rosilah Hassan[2], Mahamod Ismail[3]

[1],[2]*School of Computer Science, Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia,* 43600*, Bangi, Selangor, Malaysia*

[3]*Department of Electrical, Electronics and Systems Engineering, Faculty of Engineering, Universiti Kebangsaan Malaysia,* 43600 *UKM Bangi, Selangor, Malaysia*

maha@ftsm.ukm.my[1], rosilah@ftsm.ukm.my, mahamod@eng.ukm.my

Abstract

A Mobile Ad Hoc Network (MANET) is one of the up-to-date technologies supporting communication of mobile devices. It consists of an open environment that comprises a set of mobile, decentralized, and self-organized nodes. MANET is harder to be secured than the other types of static networks. There are many types of attacks that could paralyze the life of the mobile nodes in MANET. One of the most dangerous attacks is the Denial of Service attack (DoS), which in turn could be performed through the Resource Consumption Attack (RCA) over Ad-hoc On demand Distance Vector (AODV) routing protocol. This paper analyzes and studies the RCA effecting factors on AODV performance metrics namely throughput and end-to-end delay under varying the number of connections between the source and the destination and number of RCA attackers number.

Keywords: MANET, Resource Consumption Attack, Denial of Service attack, AODV routing protocol.

1. Introduction

A mobile ad hoc network (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. MANET network is typically used in situations where there is no centralized administration or support from networking infrastructure such as routers or base stations (Giordano, 2002).

Many up-to-date researches pay attention to MANET as a new technology with specific characteristics which distinguish its environment from other types of networks. Examples of such characteristics include: 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 decentralization ,(Cayirci & Rong, 2009; Wang et al., (2008) {Cayirci, 2009, pp.457;Wang, 2008, pp.458} {Khoukhi, 2010, pp.3}. 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 mechanisms and scenarios. Hence, it is of interest to realize how a specific type of attack is performed over particular routing protocol in order to protect MANET from its violation. This paper studies the effect of resource consumption attack (RCA) on ad-hoc on demand distance vector (AODV) routing protocol performance under varying number of connections and number of RCA attackers.

2. Background and Related Work

Karlof & Wagner, (2003) introduced 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 (Agrawal et al., 2011; Cayirci & Rong, 2009)2011; Cayirci & Rong, 2009.)

Marti et al., (2000) explained how dropping packets attack could be performed over MANET. Deng et al., (2002) and Kurosawa et al., (2007) introduced an interpretation for the effects of the black hole attack on the AODV routing protocol over MANET. On the other hand, Gerhards-Padilla et al., (2007) 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 called Tactical MANET. Wallenta et al., (2010) introduced 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 routing protocol.

2.1 AODV and its Vulnerability to RCA

2.1.1 AODV Routing Protocol

In MANET, Routing is the process of exchanging information from one node to another node of the network. Due to the limited range of devices, wireless radios routing in MANETs is often throughout multi-hop. Message in MANET is usually routed via mobile intermediate devices. AODV is a well-known reactive MANET routing protocol. To handle route information, AODV

uses three various types of route packet: Route Request (RREQ), Route Repeat (RREP) and Route Error (RERR)In AODV, to find a route to destination, AODV initiates a route discovery process. In the route discovery process,(Perkins & Royer, 1999; Taneja & Kush, 2010), the source node broadcasts the route request (RREQ) packet throughout MANET nodes -as shown in Fig. 1 and sets a timer waiting for the reply. A RREQ packet contains routing information such as the originator IP address, the broadcast ID, and the destination sequence number. Each intermediate node receives an 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. 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 unicasts 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 Fig. 2.

When a failed link is detected within the network, the intermediate nodes send RERR packet to the source node indicating which channel has failed. The source node then initiates another route discovery process to find a new route to the destination.

Fig.1. *Propagation of RREQ packet in AODV routing protocol*

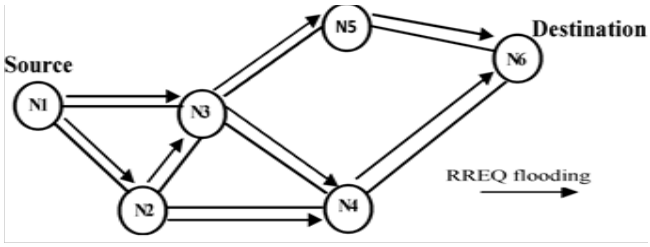
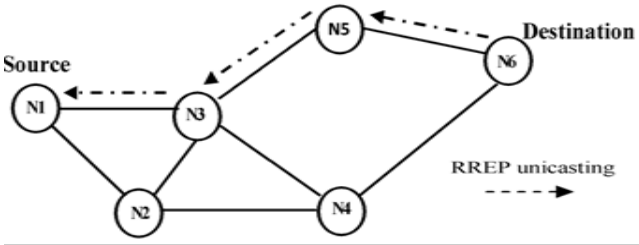


Fig.2. *The path of RREP packet in AODV routing protocol*



2.1.2 AODV and RCA

RCA (Agrawal, et al., 2011), as shown in Fig. 3 keeps the RREQ packet with a different broadcast ID in order to notify each node by broadcasting (flooding) (Ghazali & Hassan, 2011) RREQ packet continuously and consume the node' limited resource of energy and memory in addition to the link bandwidth.

As noticed, the attacker does not follow AODV rules. Therefore, to achieve its attack successfully, RCA does not set a timer waiting for a reply but keeps overflowing the network with RREQ packets. MANET is very vulnerable to this type of attack since its limited bandwidth capacity simplifies overflowing the link very easily and quickly. When MANET links have overflowed with malicious packets, the links would be jammed and congested which leads to interrupt accessing services of the available servers in MANET. In Fig. 4, if node N1 represents a server, then its service could be isolated by the attacker N3.

Fig.3. *RREQ broadcasted by RCA*

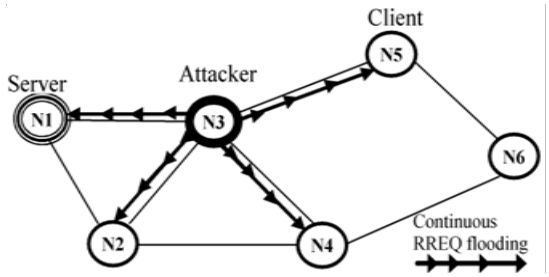
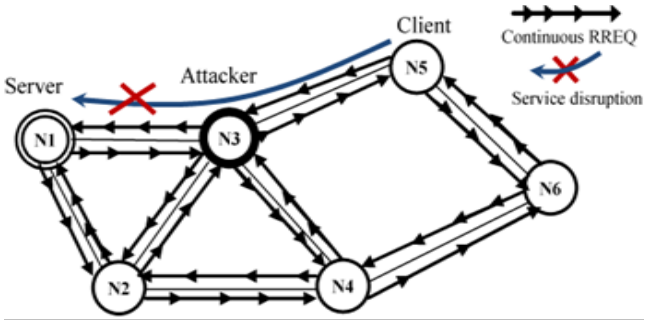


Fig.4. *Service disruption in RCA*



2.2 RCA Impact Factors Analysis

It is apparent that the basic aim behind RCA is to break the availability of MANET resources. This aim is performed by exploiting the broadcast mechanism in AODV routing protocol; in specific, the capability of the intermediate nodes to rebroadcast the RREQ packets to their neighbors. However, there are many scenarios through which RCA could perform their destroying operations. These scenarios are affected by different factors which have the primary role in making RCA either to succeed or fail. The effectiveness of RCA measures its capability to achieve its attacking successfully. On the other hand, the efficiency of RCA measures the resources used to perform its attack (Wallenta, et al., 2010). In the following, we present different factors which control the impacts on both the effectiveness and efficiency for RCA:

- Group and individual attack: In group attack, more than one attacker inject MANET with faked RREQ packets. Whilst in individual attack, only one attacker performs that destroying action. Using group attack increases the possibility to succeed the attack very quickly especially in large scale MANETs. However, using more than one attacker means consuming more than one

node resources and capabilities (energy, processing) and link bandwidth). Hence, in small scale MANET, one attacker is enough to paralyze the communication traffics between nodes without broadcasting useless faked RREQ packets.

- The number of attacker's neighbors: since RCA depends on broadcasting mechanism, the attacker with more neighbors has the opportunity to rebroadcast its faked RREQ packets more quickly than the one with fewer neighbors. Also, Group attackers with a high number of surrounding neighbors for each increase the attacking effectiveness even in large scale networks. But, if MANET is protected by a cooperative intrusion detection system (IDS) then those neighbors could reveal the attack and stop it as well (by informing the other nodes about the attacker's IP address to isolate from MANET).
- The position of the attacker: if RCA has certain target node to isolate it from MANET, or if the attacker has certain communication traffic to paralyze, then it should be close enough to the victim, else the attack operation would not be efficient or effective. Otherwise, if the attacker aims to paralyze the whole MANET, then it would be more efficient and effective if it could surround itself by more neighbors.
- The rate of broadcasted RREQs: the rate of broadcasted RREQ packets is the number of broadcasted RREQs per unit of time. Clearly, if the attacker broadcasts high number of faked RREQ packets within very close period of times, it will early success the attack. However, this scenario decreases the efficiency of the attacker; since it may broadcast useless RREQ packets which are not required in the attack. In addition, this operation may consume most of its energy very quickly. Also, receiving high rate of RREQ by normal nodes could be easily detected by their IDSs. In another point of view, the attacker may broadcast the faked RREQ packets in medium or low rate. In general, the less the rate of sending RREQ packets leads to less effectiveness and more efficiency of the attack operation.

3. Simulation Results

The simulations were conducted using QualNet version 5.0.2 (SNT, 2012). Table 1 shows the main fixed parameters considered in each simulation scenario. The preliminary goal of the simulations' scenarios is to assess the impact of RCA on the network performance by varying the number of attackers and the number of connections. Therefore, the number of attackers varies in the simulations' scenarios from zero to six attackers. The attackers are located in a random way that enables them to target the source node, the destination node and the path between each of them. In our simulations' results, each scenario result represents the average of three simulation runs.

Table 1. *Simulation parameters*

Table 1: Simulation parameters	
Parameter	Value
Simulation time	200 s
Number of nodes	100 without attackers
Attack rate	10 RREQs/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
Traffic model	CBR

Each certain number of attackers has been tested over two scenarios. In the first scenario, the experiments apply two separated CBR connections. And the second scenario applies four separated CBR connections. Separated CBR connection means that each source node is connected with only one destination node and vice versa. The connections in both scenarios differ from each other in the time of performing their communication. In the first scenario, the two CBR connections established their connection at 1s simulation time until the end of simulation while in second scenario, the four CBR connections established their connection at 100s until the end of simulation. However, the attackers start performing their flooding at time 2s until the end of the simulation time.

In random way point mobility model, as shown in Fig. 5, mobile node moves from its current location to a new one in a random choosing for moving speed and direction which are both chosen from predefined ranges [Speedmin, Speedmax] and $[0,2\pi]$, respectively. But any changes in the direction or speed from location to another happen after a certain period of time called "pause time". Once the time is expires, the mobile node is free to choose a new random path. This model is memoryless mobility model because it retains no knowledge concerning its previous location and the speed values.

We examined the following two performance metrics (Alsaqour et al., 2012)2012:

1.*Throughput*: number of received bits per unit of time on the destination node.

2.*End-to-end delay*: the time duration between sending the first bit of one packet from source node until receiving the last bit of that packet by destination node.

Figs 6 and 7 confirm the intuitive claim which states that the more attackers used in the network, the more destruction could achieve to paralyze its functionality. As shown in Fig. 6, using four connections achieves the lowest throughput when the number of attackers is 6. RCA degrades about 96% of the network throughput using 6 attackers if compared with the normal case in which there

are no attackers in the network. Also, Fig. 7 depicts that the average results of using 4 connections scenario outperforms the others in degrading the network throughput.

Fig. 8 insures that the max effect on the end-to-end delay achieved by the attackers over four connections when they are 6 attackers. Also, Fig. 9 depicts that applying RCA over 4 connections have the strongest effect on the normal nodes' end-to-end delay if we consider the average effect of attackers which are varied from 2 to 6.

Fig.5. *Random way point mobility model*

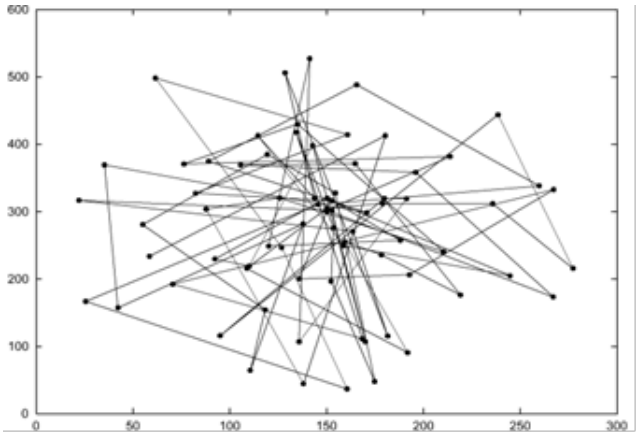


Fig.6. *RCA effect on throughput*

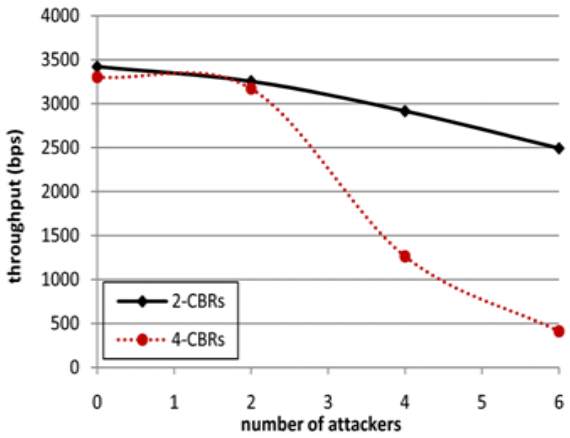


Fig.7. *The effect of the number of connections used under RCA on throughput*

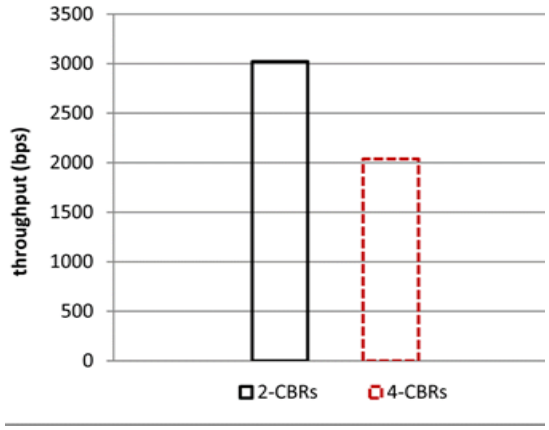


Fig.8. *RCA effect on end-to-end delay*

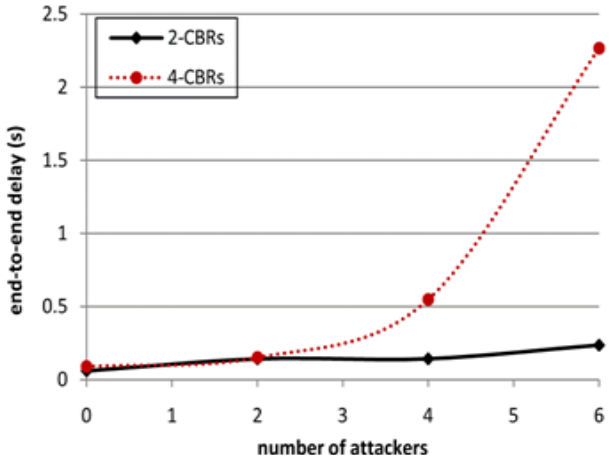
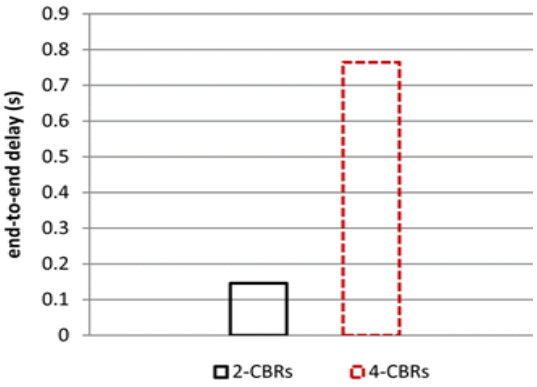


Fig.9. *The effect of the number of connections used under RCA on end-to-end delay*



4. Conclusion and Future Work

In this paper, we studied the impact of RCA on AODV routing protocol in MANET. The study focused on assessing the effect of varying the number of attackers and the number of connections on two performance metrics which are throughput and end-to-end delay. 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 energy consumption and routing packets overhead. Also, we will include more attacking scenarios such as testing the effect of attackers' radio range and flooding rate on the aforementioned metrics.

5. Acknowledgement

This research is supported by Network Communication Technology Group (NCT) http://www.ftsm.ukm. my/network/. University Kebangsaan Malaysia (UKM), 2012.

6. References

1. Agrawal S, Jain S and Sharma S (2011), A Survey of Routing Attacks and Security Measures in Mobile Ad-Hoc Networks. *Journal of Computing*, Vol.3, No.1, pp.41-48.

2. Alsaqour R A, Abdelhaq M S and Alsukour O A (2012), Effect of network parameters on neighbor wireless link breaks in GPSR protocol and enhancement using mobility prediction model, *EURASIP Journal on Wireless Communications and Networking*, 171.

3. Cayirci E and Rong C (2009), Security in wireless ad hoc and sensor networks: Wiley Online Library.

4. Deng H, Li W and Agrawal D P (2002), Routing security in wireless ad hoc networks, *IEEE Communications Magazine*, Vol.40, No.10, pp.70-75.

5. Gerhards-Padilla E, Aschenbruck N, Martini P, Jahnke M and Tolle J (2007), Detecting black hole attacks in tactical MANETs using topology graphs. Paper presented at the 32nd *IEEE Conference on Local Computer Networks*, LCN 2007.

6. Ghazali K W M and Hassan R (2011), Flooding Distributed Denial of Service Attacks-A Review, *Journal of Computer Science*, Vol.7, No.8, pp.1218-1223.

7. Giordano S (2002), Mobile ad hoc networks, *Handbook of wireless networks and mobile computing*, pp.325-346.

8. Karlof C and Wagner D (2003), Secure routing in wireless sensor networks: Attacks and countermeasures. Ad Hoc Networks, 1(2), 293-315.

9. Kurosawa S, Nakayama H, Kato N, Jamalipour A and Nemoto Y (2007), Detecting blackhole attack on AODV-based mobile ad hoc networks by dynamic learning method, *International Journal of Network Security*, Vol.5, No.3, pp.338-346.

10. Marti S, Giuli TJ, Lai K and Baker M (2000), Mitigating routing misbehavior in mobile ad hoc networks, Paper presented at the International Conference on Mobile Computing and Networking: Proceedings of the 6 th annual international conference on Mobile computing and networking.

11. Perkins C E and Royer E M. (1999), Ad-hoc on-demand distance vector routing, Paper presented at the Second IEEE Workshop on Mobile Computing Systems and Applications, WMCSA'99.

12. Scalable Network Technology (SNT). Electronic References. Retrieved Jun. 25, 2012, from http://www.scalablenetworks.com/content.

13. Taneja S and Kush A (2010), A Survey of routing protocols in mobile ad hoc networks. *International Journal of Innovation, Management and Technology*, Vol.1, No.3, pp.2010-0248.

14. Wallenta C, Kim J, Bentley P J and Hailes S (2010), Detecting interest cache poisoning in sensor networks using an artificial immune algorithm, *Applied Intelligence*, Vol.32, No.1, pp.1-26.

15. Wang D, Hu M and Zhi H (2008), A survey of secure routing in ad hoc networks. Paper presented at the The Ninth International Conference on Web-Age Information Management, WAIM'08.