Journal of Computer Science 10 (8): 1466-1472, 2014
ISSN: 1549-3636

doi:10.3844/jcssp.2014.1466.1472 Published Online 10 (8) 2014 (http://www.thescipub.com/jcs.toc)

PERFORMANCE ANALYSIS OF ADHOC ON DEMAND DISTANCE VECTOR PROTOCOL WITH BLACKHOLE ATTACK IN WSN

[1]Adnan Ahmed, [1]Kamalrulnizam Abu Bakar and
[2]Muhammad Ibrahim Channa

[1]Faculty of Computing, Universiti Teknologi Malaysia, Skudai, Johor Bahru, Malaysia
[2]Department of Information Technology,
Quaid-e-Awam University of Engg, Science and Technology, Nawabshah, Pakistan

Received 2013-11-26; Revised 2013-11-27; Accepted 2014-04-01

ABSTRACT

The security is major challenging issue in wireless sensor network applications because they are operated in public and unrestrained areas which also makes difficult to protect against tampering or captured by an adversary force that can launch insider attacks to make a node compromised. One type of such attack is black hole attack. Existing AODV routing protocol does not have mechanism to defend against such attacks. In this study, we comprehensively investigates the performance of AODV protocol by simulating it on the various network parameters with various number of blackhole nodes. The metrics for evaluation has been considered as packet delivery ratio, end to end delay, normalized routing overhead and total number of packets drop. The simulation results show that blackhole attack severely degrades the performance of WSN.

Keywords: Grayhole, Blackhole, AODV, Security, Packet Delivery Ratio

1. INTRODUCTION

The tremendous growth in wireless communication and digital electronics leads to the development of low cost and low power sensor nodes that are small in size and may communicate over short distances. Sensor networks are the type of wireless network that consists on large number of tiny sensor nodes and base stations which consist of sensing, data processing and communicating capabilities (Akyildiz *et al*., 2002). Sensor networks may have many useful and practical applications for both in military and in civilian environments. In the military application, WSN can be used for surveillance, battle field monitoring, monitoring equipment and ammunition, battle damage assessment, targeting and reconnaissance applications. In the civilian application, they can be used for environmental monitoring purposes (such as forest fire detection, flood detection, precision agriculture and earthquake prediction) and in health applications (such as telemonitoring of physiological data of elderly or chronically ill people, tracking and monitoring doctors and patients inside hospitals and drug administration). More civilian applications of sensor networks include building automation, smart environments, monitoring the status of structures, such as bridges, robot control and guidance in automatic manufacturing environments, factory process control and automation, vehicle tracking and detection, monitoring disaster area, increasing the effectiveness of agricultural processes and water management (Rassam *et al*., 2012).

The key security goals of any network, whether wired or wireless, are to protect the network against all sorts of attacks, such as eavesdropping, fabrication, injection and modification of packets and packet drop either selectively or completely. The security issues related to WSN has been raised by many researcher (Xing *et al*., 2010; Li and Gong, 2011; Manjula and Chellappan, 2012; Rathod and Mehta, 2011; Jatav *et al*., 2012; Gupta *et al*., 2012; Kim *et al*., 2012). As far as

Corresponding Author: Adnan Ahmed, Faculty of Computing, Universiti Teknologi Malaysia, Skudai, Johor Bahru, Malaysia Tel: +60163503962

security requirement for WSN is concerned, it must ensure integrity and confidentiality of data and control messages exchanged between sensors and base stations. Availability is also a significant requirement especially when the sensor network is used in real time and life critical applications, such as earthquake prediction and telemonitoring of people's health conditions.

Sensor nodes are deployed in hazards or hostile environment in large numbers, which makes their physical protection against tampering difficult or more prone to overtaking by an adversary force. By doing that adversary can learn content of memory, can have access to valid cryptographic keys and adversary can also modify the behavior of corrupted nodes (Anandkumar and Jayakumar, 2012).

The node misbehavior issues such as blackhole, grayhole (Jain *et al*., 2012) and wormhole attack (Hababeh, 2013) are popular security threads in WSN and MANET and many researchers has proposed their solutions to counter this, but still the issue is unable to prevent completely (Tseng *et al*., 2011). In this study, our methodology is to discuss how a blackhole node makes use of AODV routing process and yields attack in routing and forwarding packets. Furthermore, we also compared the performance of network in the presence of several blackhole nodes. In order to secure the network from such attacks, one should understand the behavior of this attack. The working mechanism of blackhole attack is discussed in next section. The aim ofblackhole nodes (Manikandan and Manimegalai, 2013) is to maximize overall end to end delay and routing overhead for all the traversed nodes in active route and results in low throughput and packet delivery ratio. In recent years, various studies have been made (Usha and Bose, 2012; Jalil *et al*., 2011; Garg *et al*., 2012; Ameza *et al*., 2010; Ramachandran and Shanmugam, 2012; Ehsan and Khan, 2012) to analyze the impact of node misbehavior attacks, especially blackhole attack, on AODV routing protocol in MANET and WSN.

The rest of the paper is organized as follows:

Section 2 presents briefly the overview of AODV routing protocol, blackhole attack and simulation model used in our study. Section 3 presents the simulation results. Section 4 presents the discussion and finally, section 5 concludes the study with future implementations.

2. MATERIALS AND METHODS

2.1. Overview of AODV Protocol

Adhoc On Demand Distance Vector (AODV) (Royer and Perkins, 2000) is source initiated, reactive and loop free routing protocol which creates route between source and destination when needed. AODV differs from its counterpart proactive routing protocols since in proactive routing updates are send periodically that leads to high overhead. The major objective for the design of AODV protocol is to reduce overhead. The distinguishing characteristics that leads to the selection of AODV protocol are: It is on-demand protocol means it enables to find routes when it is desired, provides fresh/latest routes information, capable of both broadcast and unicast routing, low connection setup time, more scalable and control packet routing overhead is reduced.

Each node in AODV routing protocol maintain routing table and each routing table entry for destination contains three essential elements: The next hop, hop count and sequence number. The sequence number serves as time stamp and allows the nodes to determine how freshness of route. The node that sends highest sequence number is elected for setting up route with destination because higher sequence number is considered as more correct route information. AODV routing mechanism is composed of two modules i.e., route discovery and route maintenance (Roopak and Reddy, 2013). Route discovery make use of 2 control packets such as Route Request (RREQ) and Route Reply (RREP), while route maintenance make use of Route Error (RERR) packet. The route discovery process works in request-response fashion. When a source node needs to establish a route with destination node it broadcasts the RREQ packet to all of its reachable neighbors. If the intermediate node that received the RREQ packet is the destination node, it will reply with the RREP packet. If it is not the destination node, it will broadcast the RREQ packets to its neighbor nodes. It also remembers the reverse-route to the requesting node so that it can forward responses (RREP) to this request. This process repeats until RREQ reaches destination or a node that has a valid route to destination. The node will reply with RREP packet that will be unicast along the reverse route of intermediate nodes until it reaches RREQ originating node. At the end of RREQ-RREP cycle, a bidirectional route will be established between source and destination. When a link between source and destination nodes is breakdown due to node mobility or node failure, the broken link can be repaired locally by the node upstream, else a Route Error (RERR) message is sent to the source. Once the source receives the RERR, it reinitiates route discovery if it still requires the route.

2.2. Blackhole Attack

A blackhole attack means that a misbehaving node make use of routing mechanism of protocol and claim itself to be the most suitable candidate to forward packets to destination, but drops all the received packets instead of forwarding them to intended destination (Usha and Bose, 2012). A blackhole node exploits the weakness of route discovery mechanism of reactive protocols, such as AODV, to drop all the packets in the network. A network consisting of 6 nodes is shown in **Fig. 1**, where node1 is the source and node4 is the destination node.

In order to find fresh route to destination, intermediate nodes send route discovery packets to their neighbors. When source node sends RREQ packet, Node3 which is blackhole node, sends instantly a false responds of request packet with highest sequence number that means it has shortest and new route to the destination. Therefore node1 forward its packets through blackhole (node3) to the node4 perceiving it as valid route and destination is behind the blackhole node. Source node also rejects other RREP packets coming from other nodes. As discussed above, a malicious node most likely drop the packets, so node3's behavior can be regarded as a blackhole problem in WSN. Due to this misbehavior, node3 is capable of misrouting the packets easily. The most critical influence of this attack on network, results in severely diminishing the packet delivery ratio.

2.3. Simulation Model

The performance comparison of AODV routing protocol in presence of various number of blackhole nodes has been done using Network Simulator 2 (NS2). NS2 is an open-source and event-driven simulator developed in 1981 at University of California Berkley. NS2 has proved to be useful in studying and analyzing the dynamic nature of communication networks. NS2 has achieved tremendous popularity in network and communication research community due to its flexible design and modular nature (Issariyakul and Hossain, 2012).

The simulation model is based on 25 sensor nodes that forms a wireless senor network over a area of (500×500 m), deployed in random fashion. IEEE 802.15.4 MAC protocol is used in simulation. We have varied the number of blackhole nodes from 0,1,2 and 3. The parameters used for simulation are shown in **Table 1**. The factors like packet delivery ratio, normalized routing load, end to end delay and packet drop ratio are used to understand the effect of blackhole attack in WSN.

3. RESULTS

The simulation scenario used for comparing performance of AODV against blackhole attack is shown in the **Fig. 2**.

As mentioned in **Table 1**, there are five source nodes in the scenario as nodes 21,20,17,2 and 19, placed at different positions, while node 18 is destination node. Nodes 4, 22 and 8 are designated as blackhole nodes. Each source node starts and stops sending packets at particular time as shown in the **Fig. 3**.

The performance analysis is performed with the four conditions as follows:

- When there is no blackhole node in the network
- When 1 node is compromised (node 4 behave as blackhole node)
- When 2 nodes are compromised (node 4 and node 8 behave as blackhole nodes)
- When 3 nodes are compromised (node4, node 8 and node 22 behave as blackhole nodes)

Figure 4 shows how the normalized routing overload is affected in the presence and absence of blackhole nodes.

From the results shown in **Fig. 4**, we observer that Normalized Routing Load (NRL) continues to increase when the number of blackhole nodes increases. As WSN is resource constrained network especially in terms of energy of nodes, such increased overload may badly effects the network life time of WSN.

Figure 5 shows the delivery ratio for simple AODV and AODV with blackhole nodes.

We observe from the results shown in **Fig. 5** that Packet Delivery Ration (PDR) decreases drastically as number of blackhole nodes increases in the network. With condition i, when there is no blackhole node in the network (normal-AODV), PDR was almost 100%. With condition ii, when one of the nodes in compromised in the network, PDR decreases by 60%. As shown in **Fig. 2**, blackhole node 4 is in communication range of source nodes 20, 17, 2 and 19, therefore all the traffic from the mentioned source nodes are dropped by blackhole node 4. With condition iii and iv, where number of compromised nodes are 2 and 3 respectively, PDR ratio is almost 0%.

Table 1. Simulation parameters

Simulation parameters	Values
Simulation Area	500×500 m
Simulation Time	500 sec
Number of nodes	25
Number of source nodes	5
Number of blackhole nodes	0, 1, 2, 3
Routing protocol	AODV
Packet size	50 bytes
Application layer traffic	CBR
MAC	IEEE 802.15.4
Transport layer protocol	UDP

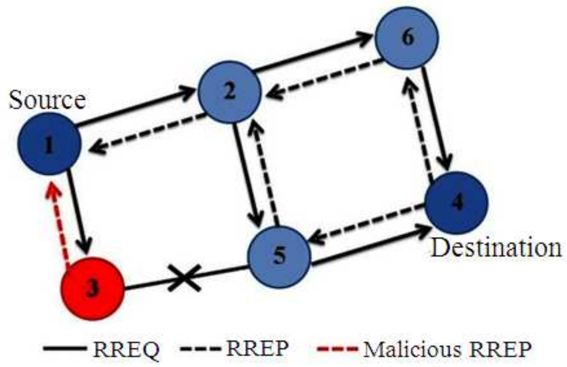

Fig. 1. Blackhole attack in WSN

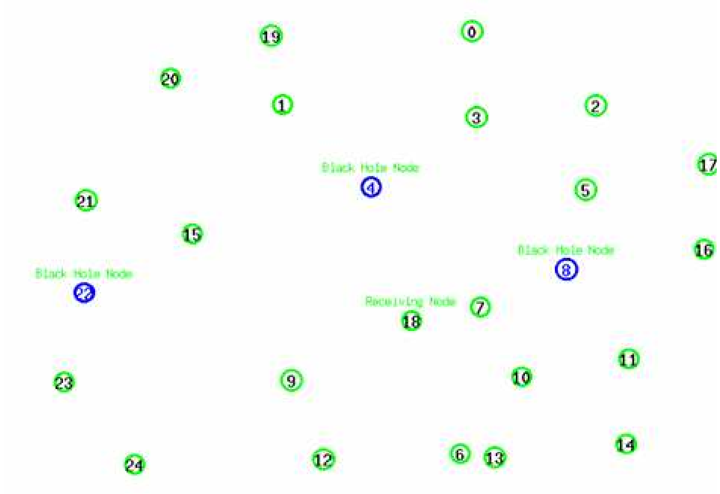

Fig. 2. Simulation scenario

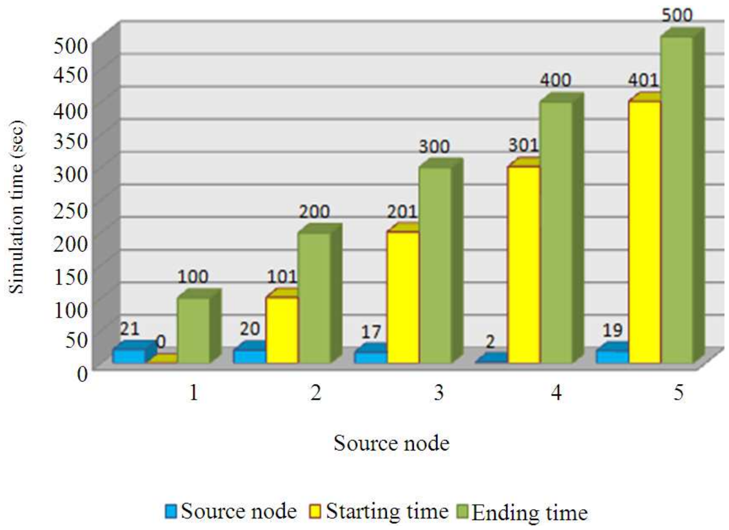

Fig. 3. Source node Vs simulation time

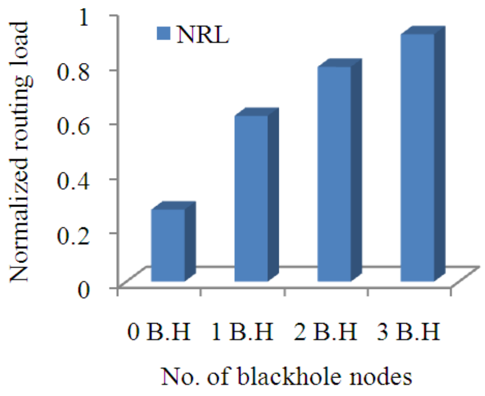

Fig. 4. No. of blackhole nodes Vs NRL

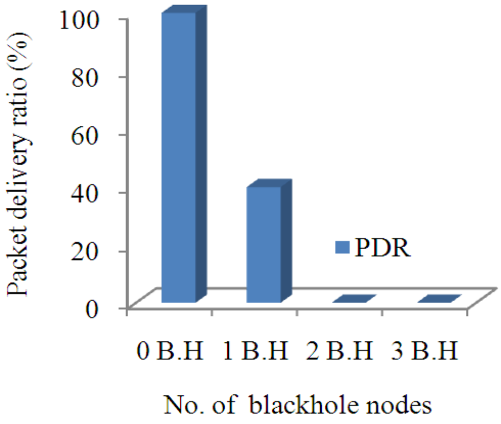

Fig. 5. No. of blackhole node Vs PDR

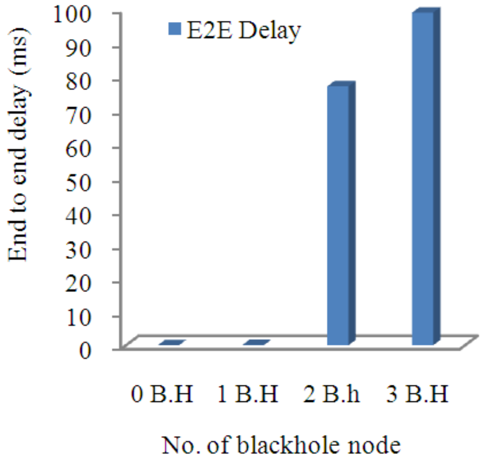

Fig. 6. No. of blackhole nodes Vs E2E delay

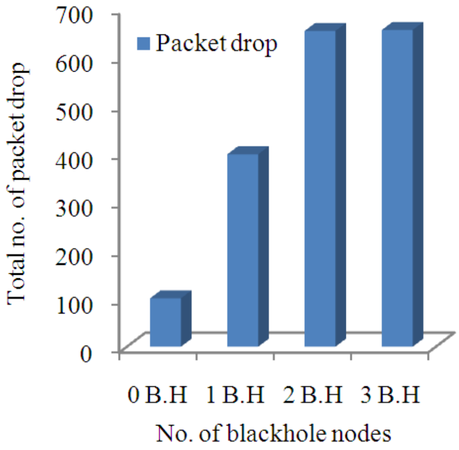

Fig. 7. No. of blackhole nodes Vs packet drop

Figure 6 shows the average end-to-end delay for the normal and compromised AODV.

From the results shown in the **Fig. 6**, we examine that End-to-End (E2E) delay increases as the number of blackhole nodes increases in the network. With condition i and ii, the E2E delay is almost same because the source node 21 is not under the effect of blackhole attack (in condition ii) and allocated simulation time is 0-100 seconds. So, it can forward the packet to destination as simulation begins. With condition iii and iv, E2E delay increases significantly (70 and 99% respectively) as most of the source nodes or all source nodes comes under the affect of blackhole attack respectively.

Figure 7 show how packet drop ratio is affected with and without blackhole nodes.

We observe from the results shown in **Fig. 7** that packet drop ratio is directly proportional to the number of blackhole nodes, as the blackhole nodes increases so do the packet drop also increases. With condition i (normal-AODV), also shows the packet drop because some of the control packets (RREQ and RREP) are dropped by the nodes due to unfreshness of route. As it is mentioned in section 2.1 that AODV makes use of sequence number in order to determine freshness of route. With condition ii (1 blackhole node), the packet drop ratio is increased by 57%. The packets from source node 21 and 17 can reach successfully at destination node because these nodes are not under the affect of blackhole attack. With condition iii and iv, the packet drop ratio almost reaches at 100%.

4. DISCUSSION

Wireless sensor network mostly operates in unattended environment without the help of any infrastructure or interaction with a human; this makes sensor networks more attractive than other networks. However, exactly this unattended and resource constrained nature of sensor networks, have led to a very demanding environment to provide security. An adversary can easily launch blackhole attack on critical sensor nodes to degrade the performance of network. Simulation results show that how badly blackhole attack affects the performance of AODV. As the number of blackhole nodes increases in the network the packet drop ratio, normalized routing load and end to end delay also increases while drastically decreases the packet delivery ratio.

5. CONCLUSION

In this study we analyzed the performance of AODV under blackhole attack. The performance analysis is carried out under different conditions with various number of blackhole nodes. We compared AODV with compromised AODV in terms of normalized routing load, packet delivery ratio, end to end delay and packet drop ratio. In this study we only simulated blackhole attack and analyzed the performance of AODV under blackhole attack. There is no such mechanism provided in this study to detect and prevent compromised nodes in AODV.

As a future work, we are planning to study the effects of other node misbehavior attacks such as grayhole, wormhole and rushing attack on AODV protocol. We also plan to design an efficient trust aware routing protocol to detect node misbehavior attacks and isolate compromised nodes from routing paths so as to improve the network performance.

6. REFERENCES

Akyildiz, I.F., W. Su, Y. Sankarasubramaniam and E. Cayirci, 2002. Wireless sensor networks: A survey. Comput. Netw., 38: 393-422. DOI: 10.1016/S1389-1286(01)00302-4

Anandkumar, K.M. and C. Jayakumar, 2012. Pro-active prevention of clone node attacks in wireless sensor networks. J. Comput. Sci., 8: 1691-1699.DOI: 10.3844/jcssp.2012.1691.1699

Ameza, F., N. Assam and R. Beghdad, 2010. Defending AODV routing protocol against the black hole attack. Int. J. Comput. Sci. Inform. Security, 08: 112-117.

Ehsan, H. and F.A. Khan, 2012. Malicious AODV: Implementation and analysis of routing attacks in manets. Porceedings of the IEEE 11th International Conference Trust, Security Privacy in Computing Communications, Jun. 25-27, IEE Xplore press, Liverpool, pp: 1181-1187. DOI: 10.1109/TrustCom.2012.199

Garg, C., P. Sharma and P. Rewagad, 2012. A literature survey of black hole attack on aodv routing protocol. Int. J. Adv.. Electron. Comput. Eng., 1: 152-157.

Gupta, C., K. Gupta and V. Gupta, 2012. Security threats in sensor network and their possible solutions. Proceedings of the International Symposium Instrumentation Measurement, Sensor Network Automation, Aug. 25-28, IEE Xplore press, Sanya, pp: 11-13. DOI: 10.1109/MSNA.2012.6324505

Hababeh, I., 2013. Performance evaluation of wormhole security approaches for ad-hoc networks. J. Comput. Sci., 9: 1626-1637. DOI: 10.3844/jcssp.2013.1626.1637

Issariyakul, T. and E. Hossain, 2012. Introduction to Network Simulator NS2. 2nd Edn., New York, ISBN-10: 1461414059, pp: 536.

Jain, A., K. Kant and M.R. Tripathy, 2012. Security solutions for wireless sensor networks. Proceedings of the 2nd International Conference Advanced Computing Communication Technologies, Jan. 7-8, IEEE Xplore press, Rohtak, Haryana, pp: 430-433. DOI: 10.1109/ACCT.2012.102

Jalil, K.A., Z. Ahmad and J.A. Manan, 2011. Mitigation of black hole attacks for aodv routing protocol. Int. J. New Comput. Architectures Applic., 2: 336-343.

Jatav, V.K., M. Tripathi, M.S. Gaur and V. Laxmi, 2012. Wireless sensor networks: Attack models and detection. Proceedings of the International Computer Science Information Technology, (SIT' 12), Singapore, pp: 144-149.

Kim, J., R.D. Caytiles and K.J. Kim, 2012. A review of the vulnerabilities and attacks for wireless sensor networks. J. Security Eng., 3: 241-250.

Li, Z. and G. Gong, 2011. A survey on security in wireless sensor networks. Department of Electrical Computer Engineering, Canada.

Manikandan, S.P. and R. Manimegalai, 2013. Trust based routing to mitigate black hole attack in manet. Life Sci. J., 10: 490-498

Manjula, V. and C. Chellappan, 2012. Trust based node replication attack detection protocol for wireless sensor networks. J. Comput. Sci., 8: 1880-1888. DOI: 10.3844/jcssp.2012.1880.1888

Ramachandran, S. and V. Shanmugam, 2012. Performance comparison of routing attacks in manet and WSN. Int. J. Ad hoc, Sensor Ubiquitous Comput., 3: 41-52.

Rassam, M.A., M.A. Maarof and A. Zainal, 2012. A survey of intrusion detection schemes in wireless sensor networks. Am. J. Applied Sci., 9: 1636-1652. DOI: 10.3844/ajassp.2012.1636.1652

Rathod, V. and M. Mehta, 2011. Security in wireless sensor network: A survey. Ganpat Unininiversty J. Eng. Technol., 1: 35-44.

Roopak, M. and B. Reddy, 2013. Black hole attack implementation in AODV routing protocol. Int. J. Scientific Eng. Res., 4: 402-406

Royer, E.M. and C.E. Perkins, 2000. An implementation study of the AODV routing protocol. Proceedings of the IEEE Wireless Communications Networking Conference, Sept. 23-28, IEEE Xplore Press, Chicago, IL., pp: 1003-1008. DOI: 10.1109/WCNC.2000.904764

Tseng, F.H., L.D. Chou and H.C. Chao, 2011. A survey of black hole attacks in wireless mobile ad hoc networks. Humancentric Comput. Inform. Sci., 1: 1-16. DOI: 10.1186/2192-1962-1-4

Usha and Bose, 2012. Comparing the impact of black hole and gray hole attacks in mobile adhoc networks. J. Comput. Sci., 8: 1788-1802. DOI: 10.3844/jcssp.2012.1788.1802

Xing, K., S.S.R. Srinivasan, M.J.M. Rivera, J. Li and X. Cheng, 2010. Attacks and countermeasures in sensor networks: A survey. Netw. Security, pp: 251-272. DOI: 10.1007/978-0-387-73821-5_11