A Survey of Solutions to Protect Against All Types of Attacks in Mobile Ad Hoc Networks

Maryam Fathi Ahmadsaraei*, Abolfazl Toroghi Haghighat

Faculty of Computer and Information Technology Engineering, Qazvin Branch, Islamic Azad University, Qazvin,Iran

Abstract

In recent years mobile networks have expanded dramatically, compared with other wireless networks. Routing protocols in these networks are designed with the assumption that there is no attacker node, so routing protocols are vulnerable to various attacks in these networks. In this paper, we review the network layer attacks and then we simulate the impact of black hole attack on ad hoc on demand distance vector routing protocol with NS-2 simulation. Then we review all kinds of intrusion detection systems (IDS) in large and small mobile ad hoc networks. We simulate these networks when they are under single black hole attack and with the existence of IDS byNS-2 simulator software. Finally, we compared the results according to throughput, packet loss ratio and packet delivery rate with each other.

Keywords: Black Hole Attack, Intrusion Detection Systems, Mobile Ad Hoc Networks, NS-2 Simulation.

1. Introduction

In Mobile ad hoc networks (MANETs) intrusion prevention and intrusion detection methods complete each other. Intrusion prevention solutions are such as encryption and authentication. When a node is captured, the attacker can achieve the encryption keys of that node. Thus encryption and authentication alone cannot defend against invaders from the network. So we should use intrusion detection methods [1].

Intrusion detection systems in fixed networks, cannot be implemented in wireless networks. In continue we will discuss about the reasons that why intrusion detection systems in ad hoc networks are challenging and complex. There is no network infrastructure in MANETs and each node can only monitor the other nodes which are in their radio range, so attackers which are out of their range can easily continue attacking the network. In ad hoc routing protocols, nodes must work together. This condition creates opportunities for attackers. Attacks in ad hoc networks are different from attacks in wired networks, so most of diagnostic methods in fixed networks are not applicable in ad hoc networks. Because of the nodes' mobility, the network configuration is dynamic and unpredictable. So the whole process of intrusion detection will become more complex. The Limit ability of nodes' computing, will restrict intrusion detection systems impacts. Because the geographical territory is not

* Corresponding author. Email: fathimaryam2000@yahoo.com

defined in ad hoc networks, securing nodes physically is so difficult. The Limit bandwidth in ad hoc networks for sending bulk intrusion detection data is challenging, in compared with wired networks [2].

Expanding the use of ad hoc networks and the importance of security in these networks has led to many studies done in this area. In [3], authors modified ad hoc on-demand distance vector (AODV) routing protocol. To guaranty security against black hole attacks they use an intrusion detection system which uses unconventional behavioral detection and expels attacker. This method increases packet delivery rate and has not overhead. In [2], authors used intrusion detection system and adaptive response method. Heads of clusters collect data from members of their clusters and store them and then send them to the node manager. Node manager uses the anti-black hole intrusion detection. Then node manager goes to next step which is called “Identifying the Attack” and then implements intrusion response. In [4], authors proposed anti-black hole algorithm. If a middle node is not the destination and does not send any route request packets yet, but forwards route reply packets, so an intrusion detector node which is close to this suspicious node should increase the suspicious of this node one unit in suspicious nodes table. If suspicious value of a node exceeded from the threshold, intrusion detector node will sent a block message to block that suspicious node. In [5], authors modified dynamic source routing protocol. In this algorithm, source node informs the destination node the number of packets that wants to send before sending data from a different path. Destination node will start counting by receiving the first packet. If the number of packets which are not received is greater than the packet loss threshold, destination will begin to identify the attacker node in that path. The proposed approach has lower packet loss rate in compare with dynamic source routing protocol. In [6], the system operates as follows: surveillance unit check out the traffic, and send suspicious data to event recording unit. With this information, attack detection unit, detect attack and inform the counter attack unit. Counter attack unit decreases the attack impacts. In [7], to encounter with unfair use of the transmission channel, nodes used digital signature to allocate a portion of their channel. To encounter with anomalies in forwarding packets authors proposed this solution: source node suspects a middle node which is away from it some hops and has the most data stream, because this suspicious node is dropping packets with unlimited rate. If suspicious counter of a node exceeded from the threshold, that node will know as an attacker. In [8], authors used cooperative and distributed methods to prevent the black hole attack. This method has four stages: The First Step: each node listens to his neighbors to know if it is reliable or not, The Second Step: is to analyze whether the suspicious node is a black hole or not, The Third Step: intrusion detector node warns to all his one hop neighbors and forces them to participate in the diagnostic process and decide whether or not the suspicious node is an attacker. The Fourth Step: there is an appropriate notification system to warn the entire network. This method has overhead. In [9], by receiving the first route response packet, source node does not choose the path and wait until all the route response packets of all the neighbors reach. Since most of the first route response packets are often from black hole nodes. In [10], authors divided the system into two parts: Local Intrusion Detection which produced a list of trusted neighbors and Global Intrusion Detection which is used to detect normal intrusions. A list of trusted neighbors is produced in local intrusion detection system. Global intrusion detection system uses this list to detect normal intrusions. In [11], if the packet forwarding rate of a node is less than the threshold, the intrusion detector node, recognizes it as a black hole node. In [12], authors present a new secure routing protocol which is based on reputation. Reputation is built on node behavior. By using incentive mechanism the possibility of activity of normal nodes increases in the network. In [13], some nodes will be chosen as check point nodes randomly. The duty of check point nodes is to send acknowledgement for each received packet. If suspicious behavior is detected, an alert packet will be sent to the source node. In [14], each node monitors his neighbors. This method leads nodes to lose a lot of energy. Nodes Judge their neighbors' behavior by comparing packet loss rate of their neighbors and defined packet loss threshold. In [15], authors proposed an adaptive intrusion detection system. If the suspicious score of a node exceeds from the threshold, intrusion detector node will isolate that node by sending a block message. In this paper, authors did not discuss about the threshold value.

In this paper we use three intrusion detection systems (IDSs) to encounter with single black hole attack. We will implement three intrusion detection systems: anomaly based intrusion detection system (ABID), Knowledge based intrusion detection system (KBID) and specification based intrusion detection system (SBID), in large and small networks which are under single black hole attack. We simulate these algorithms with network simulator (NS-2). We present the simulation environment parameters in Table 1.

In continue, in the second part we discuss about common attacks in network layer and then we simulate the impact of the black hole attack in a network which is using AODV routing protocol for routing by using NS-2 simulator. We investigate and simulate IDSs in small and large MANETs. In the third part we present conclusion and future works.

Table 1

Parameters of Simulation Environments

Parameters		Values
Simulation Area	In Small Networks	750 m X 750 m
	In Large Networks	1500 m X 300 m
Simulation Time		500 seconds
Number of Nodes	In Small Networks	19 nodes
	In Large Networks	59 nodes
Traffic Type		UDP - CBR
Packet Size		512 KB
Transmission Rate		10 Kbps
Maximum Speed		20 m/s

2. Main Content

In this section we first discuss about the types of attacks in network layer and then analyze the three types of intrusion detection systems.

2.1. Attacks in Network Layer

In an ad hoc network, nodes that are not within radio range can also communicate with each other. This feature makes ad hoc networks very flexible and vulnerable to a variety of attacks [16]. Attacks are divided into two categories: active and passive. A passive attack does not disrupt the normal operation of the network; the attacker listens to transmitted data in the network. Passive attacks are such as eavesdropping attack, traffic analysis and monitoring attack. An active attack tries to change or destroys transmitted data in the network, so the normal operation of the network will be disrupted. Active attacks are such as sleep deprivation attack, black hole attack, gray hole attack, rushing attack and Sybil attack [17].

2.1.1. Types of Passive Attacks

The purpose of eavesdropping attack is to obtain confidential information such as location, public key, private key, or password of nodes [17]. In traffic analysis and monitoring attack, the attacker monitors the transmission of packets to realize the important data of source, destination or both [17].

2.1.2. Types of Active Attacks

In sleep deprivation attack; an attacker forwards unnecessary packets to, so victim node's battery life will reduce [17]. Black hole attack is a kind of denial of service attack that the attacker node sends fake route requests packets to source node and becomes a middle node between source and destination and captures the traffic. Black hole node sends positive response to all route requests packets, even if there is no valid route to the destination. After that when source node sends data packets to the black hole node, attacker drops these packets or uses the information

[16]. In gray hole attack, attacker stops forwarding packets and aims to introduce himself as a node that has a valid route to the destination, even if the path is bogus. Then attacker drops captured packets with a special probability [17]. In rushing attack attacker receives route request packets from the source node and before receiving these packet by other nodes, attacker quickly broadcasts the packets through the network. When nodes receive route request packets from source node they assume that they are repetition packets and drop packets away. So on any route discovered by the source node, attacker is a middle node [17]. If an attacker falsifies the identity of some of the nodes that does not exist, attacker nodes conspiracy with each other which calls Sybil attack [17].

Throughput of a small network which is under black hole attack is shown in figure 3 and throughput of a large network which is under black hole attack is shown figure 6.

2.2. Intrusion Detection Systems (IDSs)

Intrusion detection is a safety technology that tries to identify nodes which want to destroy the system or take advantage of the system without having any license. An intrusion detection system monitors users and systems' behavior in the network to detect intrusion [10]. Intrusion detection systems are divided into three main categories: anomaly based intrusion detection (ABID), knowledge based intrusion detection (KBID) and specification based intrusion detection (SBID). Figure 1 shows the classification of protection methods in network layer [2].

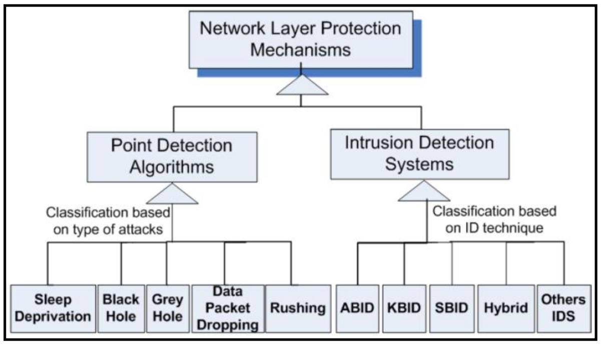
Network Layer Protection Mechanisms
Point Detection Algorithms
Intrusion Detection Systems
Classification based on type of attacks
Classification based on ID technique
Sleep Deprivation
Black Hole
Grey Hole
Data Packet Dropping
Rushing
ABID
KBID
SBID
Hybrid
Others IDS

Fig. 1. Classification of protection methods in network layer [2]

We investigate these three IDSs by three criteria: throughput, packet loss rate and packet delivery rate. So first we define these three criteria: A) Throughput: The number of bits that is transmitted from the source node to the destination node in the network communication at a unit time and usually is measured as kbps, Mbps or Gbps [3]. B) Packets Loss Rate: The number of packets which is lost (missed) to total sent packets [10]. C) Packet Delivery Rate: The number of packets that successfully reached to total sent packets [10].

In continue we investigate these three methods.

2.2.1. Anomaly Based Intrusion Detection

In anomaly based intrusion detection, normal behavior model of the network is derived and then compared this model with the network present behavior to detect intrusion in the network. In figure 2, we can see the process of Anomaly based intrusion detection system [2].

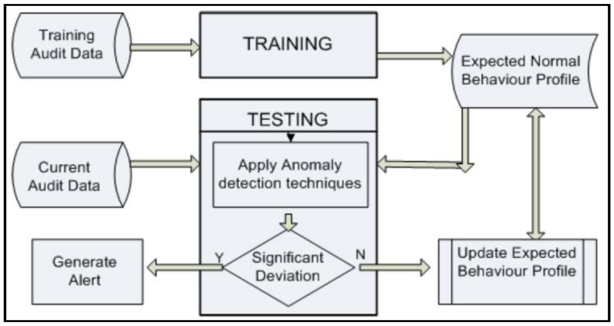
Training Audit Data
TRAINING
Expected Normal Behaviour Profile
TESTING
Current Audit Data
Apply Anomaly detection techniques
Significant Deviation
Y
N
Generate Alert
Update Expected Behaviour Profile

Fig. 2. The process of Anomaly based intrusion detection system [2]

Anomaly based intrusion detection system consists of two phases: training and testing. Training is a process to model the normal behavior of the network or users. It also acts as a user profile or network behavior. A profile contains destination features that are monitored. Building an effective profile includes collecting information about behaviors and activities that are assumed for a normal network [2]. Detection method usually involves mathematical and statistical approaches to identify any significant deviations between these two models (normal profile and present network behavior) and to detect network intrusion. Probability and statistics methods are such as Chi-Square test, Hotelling's T2 test, decision tree and Markov chain that are used for anomaly based intrusion detection systems. Neural network algorithms are used to learn and model users' behavior in the network. A key advantage of anomaly based intrusion detection systems is that they can detect new attacks and vulnerabilities, because these systems are looking for deviations from expected behavior. Of course, these systems are prone to generate false alarms [2].

In this article we use probability and statistical approach to simulate ABID in small and large networks which are under black hole attack and are equipped with ABID. The results of this simulation for a small network's throughput are shown in figure 3. Also the results of this simulation for a small network's packet loss rate and packet delivery rate are shown in figure 4. These results show that throughput and packet delivery rate in ABID is greater than KBID and SBID approaches. Also packet loss rate in ABID is smaller than KBID and SBID approaches.

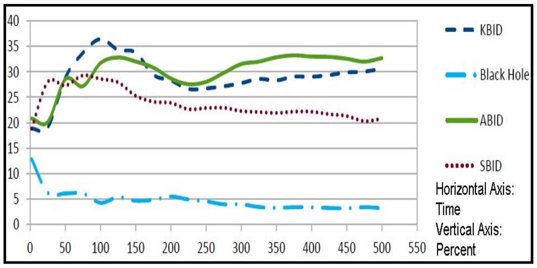

Fig. 3. Comparison chart for throughput in a small network which is under single black hole attack and nodes are equipped with different intrusion detection systems.

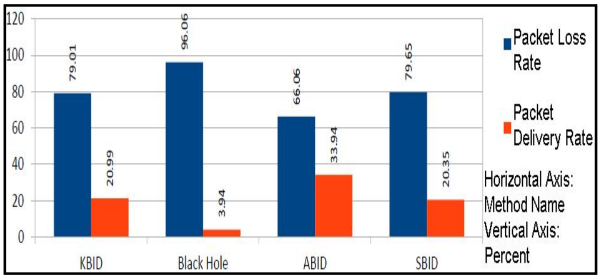

Fig. 4. Comparison Chart for packet loss rate and packet delivery rate in a small network which is under single black hole attack and nodes are equipped with different intrusion detection systems.

2.2.2. Knowledge Based Intrusion Detection

Knowledge-based intrusion detection systems keep a knowledge base that includes symptoms and known attack patterns and are seeking for these patterns to identify them. When a knowledge based intrusion detection system observes behavior like these attacks' behavior, it warns. Figure 5 shows the process of knowledge based intrusion detection system [2].

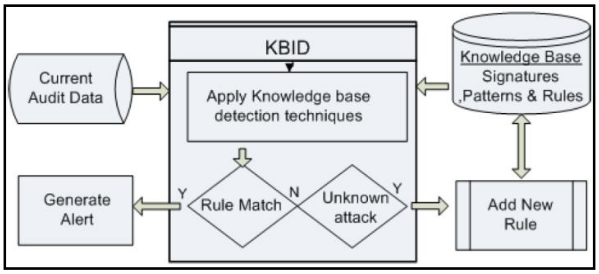

Fig. 5. The process of knowledge based intrusion detection [2]

When one or more events reduce network performance, can be identified as an attack. The reason is that this event does not match with any of the laws of attacks which are available in the knowledge base. In this way, the system can update its knowledge base. This approach uses various methods to model the knowledge base:

A) Expert Systems: Expert systems have the knowledge of known attacks in their knowledge base, as a set of rules. Data which comes from a monitoring network is translated to facts and then an inference engine uses these facts and creates a set of rules in the knowledge base to detect intrusions in the network.

B) State Transition Modeling: State transition modeling can also be used for intrusion detection where the attack presents a variety of state transition models. State transition models that represent attacks are stored in the knowledge base and are used for real time detecting intrusion in the network.

C) Rule Based Approaches: In rule based approaches known attacks are modeled as a set of rules that these rules are generated by observing or assuming methods of attack. Knowledge based intrusion detection system compares the gathered data of the network and known attacks' rules and uses forward or backward chaining methods to find evidences of the attack [2].

The main advantage of knowledge based intrusion detection system is that this method reduces false positive warns in compare with anomaly based intrusion detection system. This is because KBID only warns when it discovers behavior exactly like the pattern. So these are the best methods for a network which is so vulnerable to known attacks, although these systems can only detect attacks which have known patterns and symptoms. Also collecting and updating required information about attacks is so difficult [2].

In this article we use rule based approach to simulate KBID in small and large networks which are under black hole attack and are equipped with KBID. The results of this simulation for the throughput of small networks are shown in figure 3 and the throughput of large networks is shown in figure 6. Also the results of packet loss rate and packet delivery rate for small networks are shown in figure 4 and for large networks are shown in figure 7. The results indicate that the throughput, packet delivery rate and packet loss rate in knowledge based intrusion detection system in small and large networks are between the two approaches: anomaly based intrusion detection system and specification based intrusion detection system.

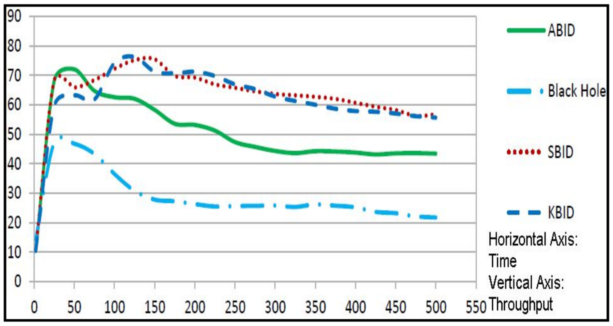

Fig. 6. Comparison Chart for throughput in a large network which is under single black hole attack and nodes are equipped with different intrusion detection systems.

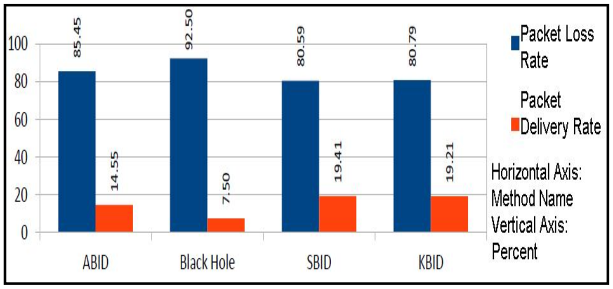

Fig. 7. Comparison Chart for packet loss rate and packet delivery rate in a large network which is under single black hole attack and nodes are equipped with different intrusion detection systems.

2.2.3. Specification based intrusion detection

In general, specification based intrusion detection systems defines the specification as a set of rules. Then use these features to monitor the routing protocol performance or network layer performance and detect attacks. The process of specification based intrusion detection is shown in figure 8 [2].

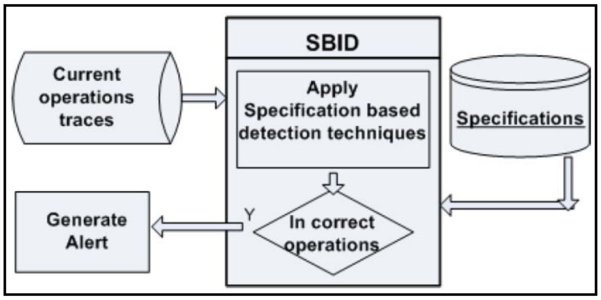
SBID
Current operations traces
Apply Specification based detection techniques
Specifications
Generate Alert
Y
In correct operations

Fig. 8. The process of specification based intrusion detection [2]

Fig. 9. First, some characteristics are extracted as a set of restrictions which define the correct functioning of the routing protocol. Then the system starts

monitoring; the deviations from these features are known as intrusion [2].

In this article we use the limitation in sequence number and the standard behavior of AODV routing protocol to simulate SBID in small and large networks which are under black hole attack and are equipped with SBID. The results of this simulation for throughput of large networks are shown in figure 6. Also the results for packet loss rate and packet delivery rate for large networks are shown in figure 7. The results show that throughput and packet delivery rate in specification based intrusion detection is greater than knowledge based intrusion detection and anomaly based intrusion detection. Also packet loss rate in specification based intrusion detection is smaller than knowledge based intrusion detection and anomaly based intrusion detection.

3. Conclusion

In this paper, we investigate and simulate large and small networks which are under single black hole attack and nodes are equipped with different intrusion detection systems. The results show that anomaly based intrusion detection systems have a good performance in small networks and specification based intrusion detection systems have a good performance in large networks. Also knowledge based intrusion detection systems have equal performance in small and large networks. It means that KBID systems have higher performance than SBID systems and lower performance than ABID systems in small networks; and have higher performance than ABID systems and lower performance than SBID systems in large networks.

Because of implementing intrusion detection systems on all the nodes, network overhead is high. Therefore, it is better to implement IDSs only on some of the nodes. Other intrusion detection system approaches can be used to implement. It is also suggested to combine one of the specification based intrusion detection techniques, with one of the knowledge based intrusion detection techniques.

References

[1] H. Shahnawaz and S. Gupta, “Black Hole Attack in AODV & Friend Features Unique Extraction to Design Detection Engine for Intrusion Detection System in Mobile Ad Hoc Network”, Journal of Engineering Science and Technology, Vol. 7, 2012.

[2] A. Nadeem and M. Howarth, “An Intrusion Detection & Adaptive Response Mechanism for MANETs”, Elsevier International Journal of Ad Hoc Networks, Vol. 12, 2013.

[3] A. Bhandare, S. Patil, B. Pail, “Modified AODV Protocol to Prevent MANET Against Black Hole Attack and its Performance Analysis”, International Journal of Advanced Scientific and Technical Research, Vol. 4, 2013.

[4] A. Deepa and V. Kavitha, “A Comprehensive Survey on Approaches to Intrusion Detection System”, Elsevier International Conference on Modeling Optimisation and Computing, Vol. 19, pp. 138-149, 2012.

[5] M. Mohanapriya and I. Krishnamurthi, “Modified DSR Protocol for Detection and Removal of Selective Black Hole Attack in MANET”, Elsevier International Journal of Computers and Electrical Engineering, Vol. 3, 2013.

[6] M. Su, “Prevention of Selective Black Hole Attacks on Mobile Ad Hoc Networks Through Intrusion Detection Systems”, Elsevier International Journal of Computer Communications, Vol. 34, 2011.

[7] S. Manikantan, C. Yu, A. Tricha, “Channel – Aware Detection of Black Hole Attacks in Mobile Ad Hoc Networks”, IEEE Global Telecommunications Conference, Vol. 3, pp. 100- 116, 2009.

[8] C. She, J. Wang, H. Yang, “Intrusion Detection for Black Hole and Gray Hole in MANETs”, KSII Transactions on Internet and Information Systems, Vol. 9, pp. 70-77, 2013.

[9] S. Madhavi and H. Tai, “An Intrusion Detection System in Mobile Ad Hoc Networks”, International Journal of Security and Its Applications Vol. 2, 2008.

[10] A. Nadeem and M. Howarth, “A Survey of MANET Intrusion Detection & Prevention Approaches for Network Layer Attacks”, IEEE Communications Surveys & Tutorials, Vol. 15, 2013.

[11] M. Su, K. Chiang, W. Liao, “Mitigation of Black Hole Nodes in Mobile Ad Hoc Networks”, IEEE International Symposium on Parallel and Distributed Processing with Applications, Vol. 10, 2010.

[12] Y. Yu, G. Lei, W. Xingwei and L. Cuixiang, “Routing Security Scheme Based on Reputation Evaluation in Hierarchical Ad Hoc Networks”, Wiley International Journal of Computer Networks, Vol.5, 2010.

[13] M. Su, “A Study of Deploying Intrusion Detection Systems in Mobile Ad Hoc Networks”, Elsevier International Conference on Electronic Engineering and Computer Science, Vol. 14,pp. 214-225, 2012.

[14] B. Xiao, B. Yu, G. Chemas, “Identify Suspect Nodes in Selective Forwarding Attacks”, Elsevier International Journal of Parallel Distributed Computing, Vol.67, 2007.

[15] U. Venkanna and L. Velusamy, “Black Hole Attack and Their Counter Measure Based on Trust Management in MANET: A Survey”, IEEE International Journal of Advances in Recent Technologies in Communication and Computing, Vol. 6, 2011.

[16] K. Al–Omari and P. Sumar, "An Overview of Mobile Ad hoc Networks for the Existing Protocols and Applications", International Journal on Applications of Graph Theory in Wireless Ad hoc Networks and Sensor Networks, Vol. 2, March 2010

[17] D. Roy, B. ebdutta, C. Rituparna, “BHIDS: A New, Cluster Based Algorithm for Black Hole IDS”, Wiley International Journal of Security and Communication Networks, Vol. 11, 2010.