6

Evaluating Intrusion Detection Systems and Comparison of Intrusion Detection Techniques in Detecting Misbehaving Nodes for MANET

Marjan Kuchaki Rafsanjani
Department of Computer Engineering, Islamic Azad University Kerman Branch
Iran

1. Introduction

Mobile Ad hoc Networks (MANETs) are a new paradigm of wireless communication for mobile hosts. These networks do not need the costly base stations in wired networks or mobile switching centres in cellular wireless mobile networks. The absence of a fixed infrastructure requires mobile hosts in MANETs to cooperate with each other for message transmissions. Nodes within the radio range of each other can communicate directly over the wireless links, while those that are far apart use other nodes as relays. In MANETs, each host must act as a router too since routes are mostly multi hop. Nodes in such a network move arbitrarily, thus the network topology changes frequently and unpredictably (Sun, 2004a). MANETs have different features with respect to the wired or even standard wireless networks. Due to their open and distributed nature, lack of fixed infrastructure, lack of central management, node mobility and dynamic topology, it enables intruders to penetrate the network in different ways. On the other hand, dependency and decentralized of MANET allows an adversary to exploit new type of attacks that are designed to destroy the cooperative algorithms used in these networks (Farhan et al., 2008). Therefore, MANETS are vulnerable to different security attacks such as distortion of routing data, exhausting node resources and maliciously manipulating data traffic.

To secure a MANET in adversarial environments, an important challenging problem is how to feasibly detect and defend possible attacks, especially internal attacks (Yu et al., 2009). Prevention mechanisms, such as encryption and authentication, can be used in MANETs to decrease intrusions, but cannot eliminate them. Hence these mechanisms are not enough to have a secure MANET. So, Intrusion Detection Systems (IDSs) are used as one of the defensive ways to detect a possible attack before the system could be penetrated. In general, if prevention mechanism and intrusion detection systems are integrated, they can provide a high-survivability network.

In this chapter, we first illustrate intrusion detection systems and then discuss why wired and cellular wireless IDSs are not suitable and applicable for MANETs. Then, the classification of IDSs is discussed and their strengths and weaknesses are evaluated. The architectures proposed so far for intrusion detection systems in MANET are classified

because they are able to operate under different security situations and conditions. Misbehaving nodes in MANET are considered and then various intrusion detection techniques for detecting these nodes are introduced and compared. Finally important future research directions are indicated.

2. Intrusion Detection Systems

Intrusion detection can be defined as a process of monitoring activities in a system which can be a computer or a network. The mechanism that performs this task is called an Intrusion Detection System (IDS) (Zhou & Hass, 1999; Anantvalee & Wu, 2006). Studies show that intrusion detection techniques just like encryption and authentication systems which are the first line of defence are not enough. As the system grows in complexity their weaknesses grow causing the network security problems to grow too. Intrusion detection can be considered as a second line of defence for network security. If an intrusion is detected then an answer for preventing intrusion or minimizing the effects can be generated. There are several assumptions for developing IDS. In the first assumption, user operations and the programs are visible and in the second assumption, normal and intrusive activities in a system behave differently. So, IDS should analyze system activities and ensure whether or not an intrusion has occurred (Brutch & Ko, 2003; Kuchaki & Movaghar, 2009).

2.1 Comparison between Wired and Cellular Wireless IDSs and MAENT IDSs

Unlike conventional cellular wireless mobile networks that rely on extensive infrastructure to support mobility, MANETs do not need expensive base stations or wired infrastructure. Global trustworthiness in all network nodes is the main fundamental security assumption in MANETs. However, this assumption is not always true in reality. The nature of MANETs makes them very vulnerable to misbehaving nodes attacks (such as malicious attacks) ranging from passive eavesdropping to active interfering. Most routing protocols only focus on providing efficient route discovery and maintenance functionality and pay little attention to routing security. Very few of them specify security measures from the very beginning. The nature of MANETs makes them very vulnerable to malicious attacks compared to traditional wired networks, because of the use of wireless links, the low degree of physical security of the mobile nodes, the dynamic topology, the limited power supply and the absence of central management point.

In a network with high security requirements, it is necessary to deploy intrusion detection techniques. While most of today's wired IDSs, which rely on real-time traffic parse, filter, format and analysis, usually monitor the traffic at switches, routers, and gateways. The lack of such traffic concentration point makes traditional wired IDSs inapplicable on MANET platforms. Each node can only use the partial and localized communication activities as the available audit traces. There are also some characteristics in MANET such as disconnected operations, which seldom exist in wired networks. What's more, each mobile node has limited resources (such as limited wireless bandwidth, computation ability and energy supply, etc.), which means MANET IDSs should have the property to be lightweight. All of these imply the inapplicability of wired IDSs on the MANET platform. Furthermore, in MANETs, it is very difficult for IDSs to tell the validity of some operations. For example, the reason that one node sends out falsified routing information could be because this node is malicious, or because of the link is broken due to the physical movement of the node. All

these suggest that an IDS of a different architecture needs to be developed to be applicable on the MANET platform (Zhang & Lee, 2000; Sun, 2004a).
In general, the important differences between MANETs and wired and cellular wireless networks make it unsuitable to apply traditional wired and cellular wireless intrusion detection technologies directly to MANET intrusion detection systems.

3. Intrusion Detection Systems Classification

Intrusion detection can be classified based on audit data collection mechanism which is host based or network based. A network-based IDS, receives packets from the network and analysis it. On the other hand, host-based IDS, analyses the events taken place in application programs or the operating systems. Also, IDS can be divided into three groups based on detection techniques which have two main types and one hybrid model; Anomaly based intrusion detection system (or behaviour-based detection), misuse based intrusion detection system (or knowledge-based detection) and specification-based intrusion detection system (hybrid detection) (Brutch & Ko, 2003; Kuchaki et al., 2008b). These three broad categories of IDSs can be used on host-based and network-based intrusion detection systems. Host-based and network-based approaches have its strengths and weaknesses; they are complementary to one another. A successful IDS would be applied in both approaches. In Table 1, comparison of network-based and host-based IDSs has been shown, in case of their strengths and weaknesses to demonstrate how these two can work together to provide additional effective intrusion detection and protection (Pahlevanzadeh & Samsudin, 2007).

Network-based IDS	Host-based IDS
• Broad in scope • Examines packet headers and entire packet • Near real-time response • Host independent • Bandwidth dependent • No overload • Slow down the networks that have IDs clients installed • Detects network attacks, as payload is analyzed • Not suitable for encrypted and switches network • Does not perform normally detection of complex attacks • High false positives rate • Lower cost of ownership • Better for detecting attacks from outside and detect attacks that host-based IDS would miss	• Narrow in scope, monitor specific activates • Does not see packet headers • Responds after a suspicious entry • Host dependent • Bandwidth independent • Overload • Slow down the hosts that have IDS clients installed • Detects local attacks before they hit the network • Well-suited for encrypted and switches environment • Powerful tool for analyzing a possible attack because of relevant information in database • Low false positive rate • Require no additional hardware • Better for detecting attacks from inside and detect attacks that network-based IDS would miss

Table 1. Evaluation of network-based and host based IDSs versus their strengths and weaknesses

4. Intrusion Detection System Architectures in MANET

The network architectures for MANET with regards to its applications are either flat or multilayer. Therefore optimum network architecture for a MANET depends on its infrastructure. In flat network infrastructures, all nodes are considered equal. Thus, they are suitable for applications such as virtual classes or conferences. In multilayer infrastructures, all nodes are considered different. Nodes may be grouped in clusters, with a cluster-head node for each cluster. To communication into a cluster, nodes are in direct contact with each other. Nodes communication between clusters is performed through each cluster-head nodes. This infrastructure is suitable for military applications (Anantvalee & Wu, 2006; Kuchaki et al., 2008b).

4.1 Stand-alone Intrusion Detection Systems

In this architecture, one IDS is executed independently for each node, and the necessary decision taken for that node is based on the data collected, because there is no interaction among network nodes and therefore no data is interchanged. In addition, each node has no knowledge of the position of other nodes in that network and no alert information crosses the network. Even though, due to its limitations, they are not effective, but they can be suitable for networks where nodes are not capable of executing an IDS or where an IDS has been installed. This architecture is also more suitable for flat network infrastructure than for multilayered network infrastructure. Due to the fact that exclusive node information is not enough to detect intrusions, thus this architecture is not selected in many of the IDS for MANETs (Farhan et al., 2008; Kuchaki et al., 2008b; Anantvalee & Wu, 2006).

4.2 Distributed and Cooperative Intrusion Detection Systems

MANETs are distributed by nature and requires nodes cooperation. Zhang et al. (Zhang et al., 2003) put forward an intrusion detection system in MANET which is both distributed and dependent on nodes cooperation. Each node cooperates in intrusion detection and an action is performed by IDS agent on it. Each IDS agent is responsible for detection, data collection and local events in order to detect intrusions and generate an independent response. Even though neighbouring IDS agents cooperate with each other when there is not any convincing evidence in global intrusion detection. So, in case of some indecisive evidence, each node runs IDS agent comprised of six modules, that include local and global detection engine and response modules. To achieve better performance, they use integration approach to analyze the attack scenario entirely. However, this architecture is complex since each node maintains local and global intrusion detection mechanism, anomalies and response methods; thus storing lot of information independently, which leads to memory overhead (Samad et al., 2005). This architecture, which is similar to stand-alone IDS architecture, is more suitable for flat network infrastructure compared with multi-level infrastructure.

4.3 Hierarchical Intrusion Detection Systems

Hierarchical IDS architecture is the well developed distributed and cooperative IDS architecture and has been presented for multi-layered network infrastructure in such a way that network is divided into clusters. The cluster-heads of each cluster has more

responsibilities compared to other members, For example, sending routing packets between clusters. In this way, these cluster-heads, behave just like control points, for example switches, routers or gateways, in wired networks. The name "multi-layer IDS" is also used for hierarchical IDS architecture. Each IDS agent is performed on every member node and locally responsible for its node, for example, monitoring and deciding on the locally detected intrusions. Each cluster-head is locally in charge of its node and globally in charge of its cluster. For example, monitoring network packets and initiating a global reaction where an intrusion is detected (Kuchaki et al., 2008b; Huang & Lee, 2003b; Yingfang et al., 2007).

4.4 Mobile Agents for Intrusion Detection Systems

Mobile agents are intelligent and autonomous agent that can move through heterogeneous network and interact with nodes. In order to employ mobile agents for intrusion detection in the network, it is necessary that many host and network devices must be installed with a mobile agent platform (Pahlevanzadeh & Samsudin, 2007). Mobile agents have been deployed in many techniques for IDSs in MANETs. Due to its ability of moving in network, each mobile agent is considered for performing just one special task and then one or more mobile agents are distributed amongst network nodes. This operation allows the distributed intrusion detection in the system. There are advantages for using mobile agents (Mishra et al., 2004). Some responsibilities are not delegated to every node, and so it helps in reducing the energy consumption, which is also an important factor in MANET network. It also provides for fault tolerance in such a way that if the network is segmented or some of the agents break down, they can still continue to function. In addition, they can work in big and different environments because mobile agents can work irrespective of their architecture, but these systems require a secure module that enables mobile agents to settle down. Moreover, Mobile agents must be able to protect themselves from secure modules on remote hosts.

For instance, Li et al. (Li et al., 2004) used the mobile agent technology for coordinated IDS in ad-hoc networks. This architecture uses the cluster-head as manager that contains assistant and response mobile agents, while each node runs a host monitor agent to detect network, file, and user intrusion using intrusion analyzer and interpretation base. The assistant agent is responsible for collecting the data from the cluster-member nodes, while the response agent is used for informing the cluster-member nodes about a certain response. It does not use the multilayer detection approach. Also, it does not use the clustering approach to minimize the intrusion response flooding (Samad et al., 2005).

Therefore the main mobile agent's features which illustrate straight relation to the special challenging requirements found in MANET include: (Hijazi & Nasser, 2005; Pahlevanzadeh & Samsudin, 2007, Kuchaki et al., 2008b)

- Robustness and fault-tolerant behaviour
- Bandwidth conservation
- Energy consumption reduction
- Load balancing improvement in the network
- Total tasks completion time reduction
- Working on a heterogeneous network
- Lightweight

These qualities make mobile agents a choice for security framework in MANET (Smith, 2001; Albers et al., 2002; Kachirski & Guha, 2002; Huang & Lee, 2003b). Data collection, data analysis, alert and alarm messages can be achieved by using mobile agents, which may reduce the data transmission to save the bandwidth resource in the MANET.

5. Misbehaving Nodes in MANET

Those nodes in the network which cause dysfunction in network and damage the other nodes are called Misbehaving or Critical nodes. Mobile Ad hoc Networks (MANETs) like other wireless networks are liable to active and passive attacks. In the passive attacks, only eavesdropping of data happens; while active attacks include injecting packets to invalid destinations, deleting packets, changing the content of packets and impersonating other nodes. Certain nodes in MANETS can produce attacks which cause congestion, distribution of incorrect routing information, services preventing proper operation, or disable them (Karygiannis et al., 2006; Lima et al., 2009).

Those nodes in the network which perform active attacks to damage other nodes and cause disconnection in the network are called Malicious or Compromised nodes. Also, those nodes which do not send the received packets (used for storing battery life span to be used for their own communications) are called Selfish nodes (Kong et al., 2002; Blazevic et al., 2001). A selfish node impacts the normal network operations by not participating in routing protocols or by not sending packets. A malicious node may use the routing protocols to announce that it has the shortest route to the destined node for sending the packets. In this situation, this node receives the packets and does not send them. This operation is called "black hole" attack (Zhang & Lee, 2000; Komninos et al., 2007).

Malicious nodes stop the operation of a routing protocol by changing the routing information or by structuring false routing information; this operation is called the "wormhole" attack. As two malicious nodes create a wormhole tunnel and are connected to each other through a private link, it can be concluded that they have a detour route in the network. This allows a node to create an artificial route in the current network and shorten the normal currency of routing messages in a way that the massages will be controlled by two attackers (Kyasanur & Vaidya, 2003; Hu et al., 2004). Malicious nodes can easily perform integrity attacks by changing the protocol fields in order to destroy the transportation of the packets, to deny access among legal nodes, and can perform attacks against the routing computations. "Spoofing" is a special case of integrity attacks with which a malicious node, due to lack of identity verification in the special routing protocols, forges the identity of a legal node. The result of such an attack by malicious nodes is the forgery of the network topology which creates network loops or partitioning of the network. The lack of integrity and authentication in the routing protocols creates forged or false messages (Komninos et al., 2007; Papadimitratos et al., 2002; Sun et al., 2004b). Malicious nodes in "selective forward" attack behave like normal nodes in most of the times but selectively drop sensitive packets for the application. Such selective dropping is difficult to detect.

Selfish nodes can intensively lower the efficiency of the network since they do not easily participate in the network operations. The aim of a selfish node is to make use of the benefits of participating in the ad hoc network without having to expand its own resources in exchange (Lima et al., 2009).

6. Intrusion Detection Techniques for Misbehaving Nodes in MANET

As it has been said before, MANETs have no infrastructure, so each node is dependant on cooperation with other nodes for routing and forwarding packets. It is possible that intermediate nodes agree for packet dispatch, but if these nodes are misbehaving nodes, they can delete or alter packets. Simulations that Marti (Marti et al., 2000) performed show that only a few misbehaving nodes can reduce entire system efficiency.

6.1 Watchdog and Pathrater

These two techniques were presented by Marti, Giuli, Lai and Baker (Marti et al., 2000) and were added to the standard routing protocol in ad hoc networks. The standard is Dynamic Source Routing protocol (DSR). Malicious nodes are recognized by eavesdropping on the next hop through Watchdog technique. Then Pathrater would help in finding the possible routes excluding the misbehaving nodes. In DSR protocol, routing data is defined in the source node. This data is passed to the intermediate nodes in the form of a message until it reaches its intended destination. Therefore each intermediate node in the path must recognize the node in the next hop. In addition, due to the special features of wireless networks, it is possible to hear messages in the next hop. For example, if node A is in the vicinity of node B, then node A can hear node B's communications. Figure 1 shows how the Watchdog technique operates.

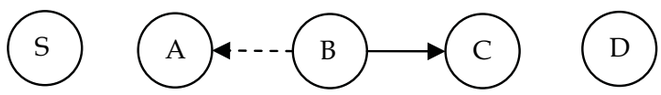

Fig. 1. Watchdog operation

Assume that node S wishes to send a packet to node D. There exists a route form S to D via A, B and C. Imagine now that node A had previously received a packet on route from S to D. The packet contains a message plus routing data. When A sends this packet to B, it keeps a copy of it in its buffer. It then eavesdrops on node B ensuring that B forwards the packet to C. If the packet is heard by B (shown by dotted lines) and it is also identical to what it has in its buffer, this indicates that B has forwarded the packet to C (shown by solid lines). The packet is then removed from the source node buffer. If, on the other hand, the packet is not compared with the packet in the source node buffer in a specific time, the Watchdog adds one to the node B's failure counter. If this counter exceeds the threshold, node A concludes that node B is malicious and reports this to the source node S.

Pathrater technique calculates path metric for every path. By keeping the ratings of each node in the network, the path metric can be calculated through combining the node rating with connection reliability which is obtained from previous experience. After calculating the path metric for all accessible paths, Pathrater will select the path with the highest metric. If such link reliable data with regards to the connection were not available, the path metrics would enable the Pathrater to select the shortest path. Thus it avoids routes that have misbehaving nodes.

Simulation results show that systems using these two techniques to find their routes are very effective in detecting misbehaving nodes. But it does not deal with or punish them in

any way. These nodes can continue to use network resources and continue their usual behaviours (Kuchaki et al., 2008b).

6.2 Confidant

Bachegger and Le Boudec (Bachegger & Le Boudec, 2002) further developed the DSR protocol and devised a new protocol called CONFIDANT, which is similar to Watchdog and Pathrater. In this protocol, each node can observe the behaviour of all its neighbouring nodes that are within its radio range and learns from them. This protocol resolves the Watchdog and Pathrater problem, meaning that it does not use the misbehaving nodes in routing and not forward packets through them, so they are punished. Additionally, when a node discovers a misbehaving node, it informs all other nodes and they too do not use this node.

CONFIDANT protocol consists of monitoring system, reputation system, trust manager and path manager. Their tasks are divided into two sections: the process to handle its own observations and the process to handle reports from trusted nodes.

Since this protocol allows network nodes to send alarm messages to each other, it is therefore a good opportunity for the attackers to send false alarm messages regarding misbehaving nodes, even though this is not true (i.e. this is not a misbehaving node).

6.3 Core

Michiardi and Molva (Michiardi & Molva, 2002) proposed a technique for detecting selfish nodes. These nodes force other nodes to cooperate with them. This technique is similar to CONIDENT is based on monitoring system and reputation system. In this technique each node receives reports from other nodes. The difference between CORE and CONFIDANT is that CORE only allows positive reports to pass through, but CONFIDANT allows negative reports. This means that CORE prevents false reports. Therefore, it prevents a DoS attack which CONFIDANT can not do. When a node can not cooperate, it is given a negative rating and its reputation decreases. In contrast, a positive rating is given to a node when a positive report is received from this node and its reputation increases.

6.4 Ocean

Bansal and Baker (Bansal & Baker, 2003) proposed a protocol called OCEAN (Observation-based Cooperation Enforcement in Ad hoc Networks), which is the enhanced version of DSR protocol. OCEAN also uses a monitoring system and a reputation system. Even though OCEAN, contrary to previous methods, relays on its own observation to avoid the vulnerability of false accusation from second-hand reputation exchanges, therefore OCEAN can be viewed as a stand-alone architecture.

OCEAN divides routing misbehaviour into two groups: misleading and selfish. If a node takes part in routes finding but does not forward a packet, it is therefore a misleading node and misleads other nodes. But if a node does not participate in routes finding, it is considered as a selfish node (Anantvalee & Wu, 2006). In order to discover misleading routing behaviours, after a node forwards a packet to its neighbour, it saves the packet and if the neighbouring node tries to forward the packet in a given time period, it is monitored. It then produces a positive or negative event as its monitoring results in order to update the rating of neighbouring node. If the rating is lower than faulty threshold, neighbouring node

is added to the list of problematic nodes and also added to RREQ as an avoid-list. As a result all traffic will not use this problematic node. This node is given a specific time to return to the network because it is possible that this node is wrongly accused of misbehaving or if it is a misbehaving node, then it must improve in this time period.

6.5 Cooperative Intrusion Detection System

Huang and Lee (Huang & Lee, 2003b) proposed a cluster-based cooperative intrusion detection system, which is similar to Kachirski and Guha's system (Kachirski & Guha, 2003). In this method, an IDS is not only capable of detecting an intrusion but also reveals the type of attack and the attacker. This is possible through statistical anomaly detection.
Identification rules for discovering attacks by using statistical formulas have been defined. These rules help to detect the type of attack and in some cases the attacking node (Huang et al., 2003a). In this technique, IDS architecture is hierarchical, and each node has an equal chance of becoming a cluster-head.
Monitoring is how data is obtained in order to analyze for possible intrusions, however it consumes power. Therefore, instead of every node capturing all features themselves, the cluster-head is solely responsible for computing traffic-related statistics. This can be done because the cluster-head overhears incoming and outgoing traffic on all members of the cluster as it is one hop away (a clique: a group of nodes where every pair of members can communicate via a direct wireless link). As a result, the energy consumption of member nodes is decreased, whereas the detection accuracy is just a little worse than that of not implementing clusters. Besides, the performance of the overall network is noticeably better - decreases in CPU usage and network overhead (Anantvalee & Wu, 2006).

6.6 ExWatchdog

Nasser and Chen (Nasser & Chen, 2007) proposed an IDS called ExWatchdog which is an extension of Watchdog. Its function is also detecting intrusion from malicious nodes and reports this information to the response system, i.e., Pathrater or Routguard (Hasswa et al., 2005). Watchdog resides in each node and is based on overhearing. Through overhearing, each node can detect the malicious action of its neighbours and report other nodes. However, if the node that is overhearing and reporting itself is malicious, then it can cause serious impact on network performance.
The main feature of the proposed system is its ability to discover malicious nodes which can partition the network by falsely reporting other nodes as misbehaving and then proceeds to protect the network. So, ExWatchdog solves a fatal problem of Watchdog.

7. Intrusion Detection Techniques Comparison for Detecting Misbehaving Nodes

The Watchdog has been used in all of the discussed IDSs, but has several limitations and in case of collisions can not work correctly and lead to wrong accusations. When each node has a different transfer range or implements directional antennas, the Watchdog can not monitor the neighbouring nodes accurately. All IDSs discussed so far can identify selfish nodes. CORE can not detect malicious nodes misbehaviours, but others can detect some of them

such as unusually frequent rout update, header change, or payload of packets, etc (Anantvalee & Wu, 2006; Kuchaki et al., 2008b).
Several mechanisms have been proposed for securing data forwarding. CORE and CANFIDANT are examples of reputation systems that provide information to distinguish between a trustworthy node and a misbehaving node. This information also encourages nodes to participate in the network in a trustworthy manner (Lima et al., 2009). Type of data collection in all the mentioned intrusion detection techniques is reputation, but in cooperative IDS technique it is statistical. Table 2 represents the final comparison among discussed IDSs.

ID Techniques		Watchdog/ Pathrater	CONFIDANT	CORE	ExWatchdag	OCEAN	Cooperative IDS
Observation	self to neighbour	yes	yes	yes	yes	yes	yes
	neighbour to neighbour	no	yes	no	no	yes	yes
Misbehavior detection	malicious - routing	no	yes	no	yes	no	yes
	malicious- packet forwarding	yes	yes	no	yes	no	yes
	selfish - routing	no	yes	yes	no	yes	yes
	selfish - packet forwarding	yes	yes	yes	yes	yes	yes
Punishment		no	yes	yes	no	yes	n/a
Avoid misbehaving node in rout finding		no	yes	no	no	yes	n/a
Architecture		Distributed and cooperative				Stand alone	Hierarchical

Table 2. Intrusion detection techniques comparison

8. Future Research Directions

In general, security research in MANET focused on Prevention to avoid any type of attack as first defence line, Intrusion Detection Systems (IDS) to detect any intruder as second defence line and Intrusion Tolerance (IT) as third defence line. The systems which use techniques for tolerating intrusions and attacks are called Intrusion Tolerance Systems (ITS) (Lima et al, 2009).
IDS research for MANETs requires a distributed architecture and the collaboration of a group of nodes to make accurate decisions. Intrusion detection techniques also should be integrated with existing MANET application. This requires an understanding of deployed applications and related attacks to deploy suitable intrusion detection mechanisms. Also attack models must be carefully established. On the other hand, solutions must consider resource limitations such as energy (Kuchaki & Movaghar, 2008a; Kuchaki & Movaghar, 2009). Sometimes the attackers may try to attack the IDS system itself. Therefore, protection against such attacks should be extended further. Also, in an extensive sense, intrusion tolerance techniques can be considered, so that these techniques can provide the development of survivable systems.

9. Conclusion

A Mobile Ad hoc Network (MANET) is a group of wireless nodes that can be dynamically organized as a multi-hop packet radio network. MANETs are an increasingly promising

area for research with lots of practical applications. However, MANETs are extremely vulnerable to attacks due to their dynamically changing topology, absence of conventional security infrastructures and open medium of communication, which unlike their wired counterparts, cannot be secure. Security issue is becoming a main concern in the applications of MANET. We considered the problem of misbehaving nodes and detecting them by Intrusion Detection techniques in Mobile Ad hoc Networks.

Experience has shown that avoidance techniques such as cryptography and authentication are not enough. Therefore, intrusion detection systems have grown popular. With respect to MANET features, nearly all of the IDSs are distributed and have a cooperative architecture. New attacks are growing quickly and they have to be detected before any damage is caused to the system or data. The aim of an intrusion detection system is detecting attacks on mobile nodes or intrusions into network. Intrusion detection systems, if designed well, can effectively identify misbehaving activities and help to offer adequate protection. Therefore, an IDS has become an indispensable component to provide defence-in-depth security mechanisms for MANETs.

Some attacks are also categorized as misbehaviour attacks, being generated by network nodes whose actions cannot be trusted or do not conform to protocol specifications. Black hole, wormhole, flooding and selective forwarding are examples of misbehaviour attacks which are created by misbehaving nodes such as malicious and selfish nodes in the network. So, techniques in mobile ad hoc networks with wireless channel have been proposed to detect and minimize misbehaving nodes. On the other hand, intrusion detection techniques used in wired networks cannot be directly applied to mobile ad hoc networks due to special characteristics of the networks. Furthermore, most current MANET intrusion detection systems are still in the test phase.

10. References

Albers, P.; Camp, O.; Percher, J.; Bernard, J.; Ludovic, M. & Puttini, R. (2002). Security in ad hoc networks: A general intrusion detection architecture enhancing trust based approaches, *Proceedings of the 1st International workshop on Wireless Information systems*, pp. 3-6, Ciudad Real, Spain.

Anantvalee, T. & Wu, J. (2006). A survey on intrusion detection in mobile ad hoc networks, In : *Wireless/Mobile Network Security*, Xiao, Y.; Shen, X. & Du, D.-Z., page numbers (170-196), Springer.

Bansal, S. & Baker, M. (2003). Observation-based cooperation enforcement in ad hoc networks, *Research Report cs.NI/0307012 vl*, July 2003, Stanford University.

Blazevic, L.; Buttyan, L.; Capkun, S.; Giordano, S.; Hubaux, J. & Le Boudec J. (2001). Self-organization in mobile ad-hoc networks: The approach of terminodes, *IEEE Communications Magazine*, Vol. 39, No. 6, June 2001, page numbers (166–174).

Brutch, P. & Ko, C. (2003). Challenges in intrusion detection for wireless ad-hoc networks, *Proceedings of the Symposium on Applications and the Internet Workshops*, pp. 368-373, ISBN: 0-7695-1873-7, January 2003.

Buchegger, S. & Le Boudec, J.-Y. (2002). Performance analysis of the CONFIDANT protocol: Cooperation of nodes - fairness in dynamic ad-hoc networks, *Proceedings of the IEEE/ACM Workshop on Mobile Ad Hoc Networking and Computing (MobiHoc'02),* pp.226-336, Lausanne, Switzerland, June 2002.

Farhan, A.F.; Zulkhairi, D. & Hatim, M.T. (2008). Mobile agent intrusion detection system for mobile ad hoc networks: A non-overlapping zone approach, *Proceedings of the 4th IEEE/IFIP International Conference on Internet(ICI)*, pp. 1-5, ISBN: 978-1-4244-2282-1, Tashkent, September 2008.

Hasswa, A.; Zulkernine, M. & Hassanein, H. (2005). Routeguard: an intrusion detection and response system for mobile ad hoc networks, *Proceedings of the IEEE International Conference on Wireless and Mobile Computing, Networking And Communication*, Vol. 3, pp. 336-343, ISBN: 0-7803-9181-0, August 2005.

Hijazi, A. & Nasser, N. (2005). Using mobile agents for intrusion detection in wireless ad hoc networks, *proceedings of the second IFIP International Conference on Wireless and Optical Communications Networks(WOCN2005),* pp. 362-366, ISBN: 0-7803-9019-9, March 2005.

Hu, Y.-C.; Perrig A. & Johnson D.B. (2003). Packet leashes: A defense against wormhole attacks in wireless networks, *Proceedings of the 22th Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM'03)*, Vol. 3, pp. 1976-1986, ISBN: 0-7803-7752-4, March/April 2003.

Huang, Y.; Fan, W.; Lee, W. & Yu, P. (2003a). Cross-feature analysis for detecting ad-hoc routing anomalies, *Proceedings of the 23rd IEEE International Conference on Distributed Computing Systems (ICDCS'03)*, pp. 478-487, May 2003.

Huang, Y. & Lee, W. (2003b). A cooperative intrusion detection system for ad hoc networks. *Proceedings of the 1st ACM Workshop on Security of Ad Hoc and Sensor Networks,* pp. 135-147, ISBN: 1-58113-783-4, Fairfax, Virginia.

Kachirski, O. & Guha,R. (2002). Intrusion detection using mobile agents in wireless ad hoc networks, *Proceedings of the IEEE Workshop on Knowledge Media Networking*, pp. 153-158, ISBN: 0-7695-1778-1.

Kachirski, O. & Guha, R. (2003). Effective intrusion detection using multiple sensors in wireless ad hoc networks, *Proceedings of the 36th Annual Hawaii International Conference on System Sciences (HICSS'03)*, pp. 57.1, ISBN: 0-7695-1874-5, January 2003.

Karygiannis, A.; Antonakakis, E. & Apostolopoulos, A. (2006). Detecting critical nodes for MANET intrusion detection systems, *Proceedings of 2nd International Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing*, pp. 9-15, ISBN: 0-7695-2549-0, Lyon, June 2006.

Komninos, N.; Vergados, D. & Douligeris C. (2007). Detecting unauthorized and compromised nodes in mobile ad hoc networks, *Elsevier Ad hoc network Journal*, Vol. 5, No. 3, April 2007, page numbers (289-298), ISSN: 1570-8705.

Kong, J.; Luo, H.; Xu, K.; Gu, D.L.; Gerla, M. & Lu, S. (2002). Adaptive security for multi-level ad hoc networks, *Wireless Communication and Mobile Computing Journal*, Vol. 2, No. 5, September 2002, page numbers (533-547).

Kuchaki Rafsanjani, M. & Movaghar, A. (2008a). Identifying monitoring nodes in MANET by detecting unauthorized and malicious nodes, *Proceedings of the 3rd IEEE International Symposium on Information Technology (ITSIM'08)*, pp. 2798-2804, ISBN: 978-1-4244-2327-9, Kuala Lumpur, Malaysia, August 2008.

Kuchaki Rafsanjani, M.; Movaghar, A. & Koroupi, F. (2008b). Investigating intrusion detection systems in MANET and Comparing IDSs for detecting misbehaving

nodes, *Proceedings of World Academy of Science, Engineering and Technology*, Vol. 34, pp. 351-355, ISSN: 2070-3740, Venice, Italy, October 2008.

Kuchaki Rafsanjani, M. & Movaghar, A. (2009). Developing a hybrid method for identifying monitoring nodes in intrusion detection systems of MANET. *Contemporary Engineering Sciences Journal*, Vol. 2, No. 3, page numbers (105-116), ISSN: 1313-6569.

Kyasanur, P. & Vaidya, N.H. (2003). Detection and handling of MAC layer misbehavior in wireless networks, *Proceedings of International Conference on Dependable Systems and Networks (DSN'03)*, pp. 173–182, ISBN: 0-7695-1952-0, June 2003.

Li, C.; Song, Q. & Zhang, C. (2004). MA-IDS architecture for distributed intrusion detection using mobile agents, *Proceedings of the 2nd International Conference on Information Technology for Application (ICITA)*, pp. 451-455, ISBN: 0-646-42313-4.

Lima, M.N.; Santos, A.L. & Pujolle, G. (2009). A survey of survivability in mobile ad hoc networks, *IEEE Communications Surveys & Tutorials Journal*, Vol. 11, No. 1, First Quarter 2009, page numbers (66- 77), ISSN: 1553-877X.

Marti, S.; Giuli, T.J.; Lai, K. & Baker, M. (2000). Mitigating routing misbehavior in mobile ad hoc networks, *Proceedings of the 6th Annual International Conference on Mobile Computing and Networking (MobiCom'00),* pp. 255-265, ISBN: 1-58113-197-6, Boston, Massachusetts, United States, August 2000.

Michiardi, P. & Molva, R. (2002). CORE: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks, *Proceedings of the IFIP TC6/TC11 Sixth Joint Working Conference on Communications and Multimedia Security*, pp. 107-121, ISBN: 1-4020-7206-6, Deventer, The Netherlands, September 2002.

Mishra, A.; Nadkarni, K. & Patcha, A. (2004). Intrusion detection in wireless ad hoc networks, *IEEE Wireless communication Journal,* Vol. 11, No. 1, February 2004, page numbers (48-60), ISSN: 1536-1284.

Nasser, N. & Chen, Y. (2007). Enhanced intrusion detection system for discovering malicious nodes in mobile ad hoc network, *Proceedings of the IEEE International Conference on Communication (ICC'07),* pp. 1154-1159, ISBN: 1-4244-0353-7, Glasgow, June 2007.

Pahlevanzadeh, B. & Samsudin, A. (2007). Distributed hierarchical IDS for MANET over AODV+, *Proceedings of the IEEE International Conference on Telecommunications and Malaysia International Conference on Communications*, pp. 220-225, ISBN: 978-1-4244-1094-1, Penang, Malaysia, May 2007.

Papadimitratos, P.; Haas, Z.J. & Sirer, E.G. (2002). Path set selection in mobile ad hoc networks, *Proceedings of the 3rd ACM International Symposium on Mobile Ad Hoc Networking and Computing*, pp. 1–11, ISBN: 1-58113-501-7, Lausanne, Switzerland.

Samad, K.; Ahmed, E.; Mahmood, W.; Sharif, K. & Chaudhry, A.A. (2005). Efficient clustering approach for intrusion detection in ad hoc networks, *Proceedings of Conference on Engineering Sciences and Technology*, pp. 1-6, ISBN: 978-0-7803-9442-1, Karachi, August 2005.

Smith, A. (2001). An examination of an intrusion detection architecture for wireless ad hoc networks, *Proceedings of the 5th National Colloquium for Informayion System Security Education*, May 2001.

Sun, B. (2004a). *Intrusion Detection in Mobile Ad Hoc Networks* (Dissertation), ProQuest Information and Learning Company, UMI Number: 3172171, USA.

Sun, B.; Kui W.; & Pooch, U.W. (2004b). Towards adaptive intrusion detection in mobile ad hoc networks, *Proceedings of the IEEE Global Telecommunications Conference*

(GLOBECOM'04), Vol. 6, pp. 3551–3555, ISBN: 0-7803-8794-5, November/December 2004.

Yingfang, F.; Jingsha, H. & Guorui, L. (2007). A distributed intrusion detection scheme for mobile ad hoc networks, *Proceedings of the 31st Annual International Computer Software and Applications Conference (COMPSAC),* Vol. 2, pp. 75-80, ISBN: 0-7695-2870-8, Beijing, July 2007.

Yu, M.; Zhou, M. & Su, W. (2009). A secure routing protocol against byzantine attacks for MANETs in adversarial environments, *IEEE Transactions on Vehicular Technology*, Vol. 58, No. 1, January 2009, page numbers (449-460), ISSN: 0018-9545.

Zhang, Y. & Lee, W. (2000). Intrusion detection in wireless ad hoc networks, *Proceedings of the 6th Annual International Conference on Mobile Computing and Networking (ACM MobiCom'00)*, pp. 275-283, ISBN: 1-58113-197-6, Boston, Massachusetts, United States, August 2000.

Zhang, Y.; Lee, W. & Huang Y.-A. (2003). Intrusion detection techniques for mobile wireless networks, *Wireless Networks Journal (ACM WINET)*, Vol. 9, No. 5, September 2003, page numbers (545-556), ISSN: 1022-0038.

Zhou, L. & Hass, Z.J. (1999). Securing ad hoc networks. *IEEE Network Magazine Special Issue on Network Security*, Vol. 13, No. 6, November/December 1999, page numbers (24-30).

Advanced Technologies

Edited by Kankesu Jayanthakumaran

ISBN 978-953-307-009-4
Hard cover, 698 pages
Publisher InTech
Published online 01, October, 2009
Published in print edition October, 2009

This book, edited by the Intech committee, combines several hotly debated topics in science, engineering, medicine, information technology, environment, economics and management, and provides a scholarly contribution to its further development. In view of the topical importance of, and the great emphasis placed by the emerging needs of the changing world, it was decided to have this special book publication comprise thirty six chapters which focus on multi-disciplinary and inter-disciplinary topics. The inter-disciplinary works were limited in their capacity so a more coherent and constructive alternative was needed. Our expectation is that this book will help fill this gap because it has crossed the disciplinary divide to incorporate contributions from scientists and other specialists. The Intech committee hopes that its book chapters, journal articles, and other activities will help increase knowledge across disciplines and around the world. To that end the committee invites readers to contribute ideas on how best this objective could be accomplished.

How to reference

In order to correctly reference this scholarly work, feel free to copy and paste the following:

Marjan Kuchaki Rafsanjani (2009). Evaluating Intrusion Detection Systems and Comparison of Intrusion Detection Techniques in Detecting Misbehaving Nodes for MANET, Advanced Technologies, Kankesu Jayanthakumaran (Ed.), ISBN: 978-953-307-009-4, InTech, Available from: http://www.intechopen.com/books/advanced-technologies/evaluating-intrusion-detection-systems-and-comparison-of-intrusion-detection-techniques-in-detecting

INTECH
open science | open minds

InTech Europe
University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia
Phone: +385 (51) 770 447
Fax: +385 (51) 686 166
www.intechopen.com

InTech China
Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元
Phone: +86-21-62489820
Fax: +86-21-62489821

IntechOpen