A Survey on MANET Intrusion Detection

Satria Mandala satriamandala@hotmail.com
Faculty of Science & Technology
Department of Informatics Engineering
State Islamic University of Malang
Jl. Gajayana 50 Malang, Indonesia

Md. Asri Ngadi dr.asri@utm.my
Faculty of Computer Science & Information System,
Department of Computer System & Communication
Universiti Teknologi Malaysia (UTM)
Skudai - Johor, 81310, Malaysia

A. Hanan Abdullah hanan@utm.my
Professor, Faculty of Computer Science & Information System,
Department of Computer System & Communication
Universiti Teknologi Malaysia (UTM)
Skudai - Johor, 81310, Malaysia

Abstract

In recent years, the security issues on MANET have become one of the primary concerns. The MANET is more vulnerable to be attacked than wired network. These vulnerabilities are nature of the MANET structure that cannot be removed. As a result, attacks with malicious intent have been and will be devised *to exploit* these vulnerabilities and *to cripple* the MANET operation. Attack prevention measures, such as authentication and encryption, can be used as the first line of defense for reducing the possibilities of attacks. However, these techniques have a limitation on the effects of prevention techniques in general and they are designed for a set of known attacks. They are unlikely to prevent newer attacks that are designed for circumventing the existing security measures. For this reason, there is a need of second mechanism to "detect and response" these newer attacks, i.e. "*intrusion detection*". This paper aims *to explore* and *to classify* current techniques of Intrusion Detection System (IDS) aware MANET. To support these ideas, a discussion regarding attacks, IDS architectures, and researches achievement on MANET are presented inclusively, and then the comparison among several researches achievement will be evaluated based on these parameters. By this way, several existing security problems on MANET can be probed quickly for future researches.

Keywords: Intrusion Detection System (IDS), MANET, Survey, Wireless Ad hoc Network

1. INTRODUCTION

In MANET, a set of interacting nodes should cooperatively implement routing functions to enable end-to-end communication along dynamic paths composed by multi-hop wireless links. Several multi-hop routing protocols have been proposed for MANET, and most popular ones include:

Dynamic Source Routing (DSR) [1], Optimized Link-State Routing (OLSR) [2], Destination-Sequenced Distance-Vector (DSDV) [3] and Ad Hoc On-Demand Distance Vector (AODV) [4]. Most these protocols rely on the assumption of a trustworthy cooperation among all participating devices; unfortunately, this may not be a realistic assumption in real systems. Malicious nodes could exploit the weakness of MANET to launch various kinds of attacks.

Node mobility on MANET cannot be restricted. As results, many IDS solutions have been proposed for wired network, which they are defined on strategic points such as switches, gateways, and routers, can not be implemented on the MANET. *Thus, the wired network IDS characteristics must be modified prior to be implemented in the MANET*.

The rest of this paper will be structured as follows. Section 2 describes background of the IDS. The Intrusion detection on MANET is presented on section 3. In section 4, we present a discussion regarding the IDS classification. Finally, the conclusions and future research are shown in section 5.

2. IDS BACKGROUND

An intrusion-detection system (IDS) can be defined as the tools, methods, and resources to help identify, assess, and report unauthorized or unapproved network activity. Intrusion detection is typically one part of an overall protection system that is installed around a system or device—it is not a stand-alone protection measure.

Intrusion detection has a bit more history behind it. Endorf [5] stated that the intrusion detection was introduced as a formal research when James Anderson wrote a technical report [6] for the U.S. Air Force. Thus, it has been followed by Denning [7], Heberlein [8], and many researchers until present day.

Depending on the detection techniques used, IDS can be classified into three main categories [9] as follows: 1) signature or misuse based IDS), 2) anomaly based IDS, 3) specification based IDS, which it is a hybrid both of the signature and the anomaly based IDS.

- *The signature-based IDS* uses pre-known attack scenarios (or signatures) and compare them with incoming packets traffic. There are several approaches in the signature detection, which they differ in representation and matching algorithm employed to detect the intrusion patterns. The detection approaches, such as expert system [10], pattern recognition [11], colored petri nets [12], and state transition analysis [13] are grouped on the misuse.
- Meanwhile, *the anomaly-based IDS* attempts to detect activities that differ from the normal expected system behavior. This detection has several techniques, i.e.: statistics [14], neural networks [15], and other techniques such as immunology [16], data mining [[18[, [19]], and Chi-square test utilization [17]. Moreover, a good taxonomy of wired IDSes was presented by Debar [20].
- *The specification-based* IDS monitors current behavior of systems according to specifications that describe desired functionality for security-critical entities [48]. A mismatch between current behavior and the specifications will be reported as an attack.

3. MANET INTRUSION DETECTION

There are three focuses in this section: attacks, IDS architectures grouping, and researches achievement. The “researches achievement review” uses several parameters such as the IDS architectures, the detection techniques (see section 2), the resistance to several attacks type, and the routing protocols (see section 1).

3.1 ATTACKS

The MANET is susceptible to passive and active attacks [21]. The Passive attacks typically involve only eavesdropping of data, whereas the active attacks involve actions performed by adversaries such as replication, modification and deletion of exchanged data. In particular, attacks in MANET can cause congestion, propagate incorrect routing information, prevent services from working properly or shutdown them completely [[22],[25],[26],[23],[24],[27]].

Nodes that perform the active attacks are considered to be malicious, and referred to as *compromised*, while nodes that just drop the packets they receive with the aim of saving battery life are considered to be *selfish* [[28],[26]]. A selfish node affects the normal operation of the network by not participating in the routing protocols or by not forwarding packets. In addition, a compromised node may use *the routing protocol* to advertise itself as having the shortest path to the node whose packets it wants to intercept as in the so called *black hole* attack [[29], [30]].

Spoofing is a special case of integrity attacks whereby a compromised node impersonates a legitimate one due to the lack of authentication in the current ad hoc routing protocols [[35],[36]]. The main result of the spoofing attack is the misrepresentation of the network topology that may cause network loops or partitioning. Lack of integrity and authentication in routing protocols creates *fabrication attacks* [[37],[4],[38]] that result in erroneous and bogus routing messages.

Denial of service (DoS) is another type of attack, where the attacker injects a large amount of junk packets into the network. These packets overspend a significant portion of network resources, and introduce wireless channel contention and network contention in the MANET [[39],[40]]. A *routing table overflow attack* and *sleep deprivation attack* are two other types of the DoS attacks [41]. In the routing table *overflow attack*, an attacker attempts to create routes to non-existent nodes. Meanwhile the *sleep deprivation attack* aims to consume the batteries of a victim node.

There are also more sophisticated routing attacks. Compared to the simple attacks described above, these sophisticated attacks are much harder to detect and to prevent, i.e.: *wormhole attacks* (two compromised nodes create a tunnel that is linked through a private connection and thus they by-pass the network [[31],[32]]), *rushing attacks* [33] and *sybil attacks* [34].

3.2 IDS ARCHITECTURES

Based on the network infrastructures, the MANET can be configured to either flat or multi-layer. The optimal IDS architecture for the MANET may depend on the network infrastructure itself. There are four main architectures on the network [43], as follows: 1) Standalone IDS, 2) Distributed and Collaborative IDS, 3) Hierarchical IDS, and 4) Mobile Agent for Intrusion Detection Systems.

- *In the standalone architecture*, the IDS runs on each node to determine intrusions independently. There is no cooperation and no data exchanged among the IDSes on the network. This architecture is also more suitable for flat network infrastructure than for multi-layered network infrastructure

- *The distributed and collaborative architecture* has a rule that every node in the MANET must participate in intrusion detection and response by having an IDS agent running on them. The IDS agent is responsible for detecting and collecting local events and data to identify possible intrusions, as well as initiating a response independently.

- *The hierarchical architecture* is an extended version of the distributed and collaborative IDS architecture. This architecture proposes using multi-layered network infrastructures where the network is divided into clusters. The architecture has cluster heads, in some sense, act as control points which are similar to switches, routers, or gate ways in wired networks.

- *The mobile agent for IDS architecture* uses mobile agents to perform specific task on a nodes behalf the owner of the agents. This architecture allows the distribution of the intrusion detection tasks. There are several advantages using mobile agents [[21], [42]], for intrusion detection.

3.3 RESEARCHES ACHIEVEMENT

Many researchers have proposed several IDS especially for the MANET, some of them will be reviewed in the following paragraph.

Since the nature of MANET node is *distributed* and *requires cooperation* to other nodes, ***Zhang, Lee, and Huang [[30], [24]]*** proposed "intrusion detection (ID) and response system" should follow both the natures. In this proposed architecture model, each node is responsible for detecting signs of intrusion locally and independently, but neighboring nodes can collaboratively investigate in a broader range. Individual IDS agents are placed on each and every node. Each the IDS agent runs independently and monitors local activities (user and systems activities, and communication activities within the radio range). The agent detects intrusion from local traces and initiates response. If anomaly is detected in the local data, or if the evidence is inconclusive and a broader search is warranted, neighboring IDS agents will cooperatively participate in global intrusion detection actions. These individual IDS agents collectively form the IDS system to defend the wireless ad-hoc network.

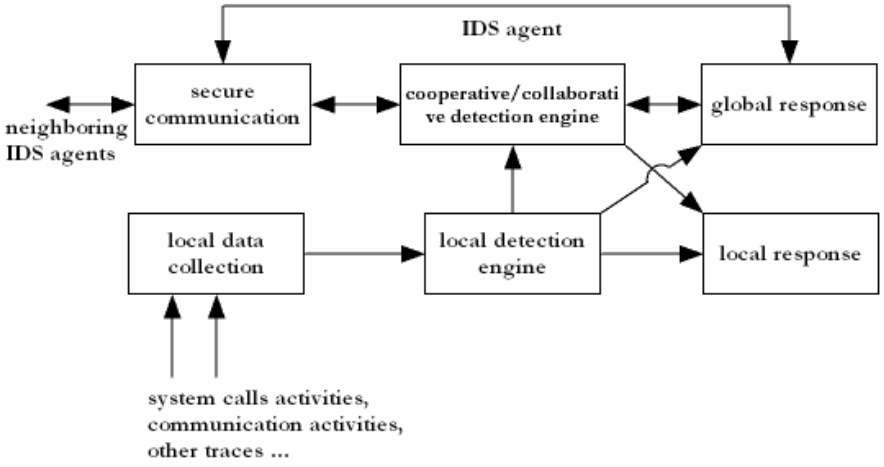

FIGURE 1: IDS agent model

Albers et al. [44] proposed a distributed and collaborative architecture of IDS by *using mobile agents*. A Local Intrusion Detection System (LIDS) is implemented on every node for local concern, which can be extended for global concern by cooperating with other LIDS. Two types of data are exchanged among LIDS: security data (to obtain complementary information from collaborating nodes) and intrusion alerts (to inform others of locally detected intrusion). In order to analyze the possible intrusion, data must be obtained from what the LIDS detects on, along with additional information from other nodes. Other LIDS might be run on different operating systems or use data from different activities such as system, application, or network activities; therefore, the format of this raw data might be different, which makes it hard for LIDS to analyze. However, such difficulties can be solved by using Simple Network Management Protocol (SNMP) data located in Management Information Base (MIBs) as an audit data source. Such a data source not only eliminates those difficulties, but also reduces the increase in using additional resources to collect audit data if an SNMP agent is already run on each node. For the methodology of detection, Local IDS Agent can use either anomaly or misuse detection. However, the combination of two mechanisms will offer the better model. Once the local intrusion is detected, the LIDS initiates a response and informs the other nodes in the network. Upon receiving an alert, the LIDS can protect itself against the intrusion.

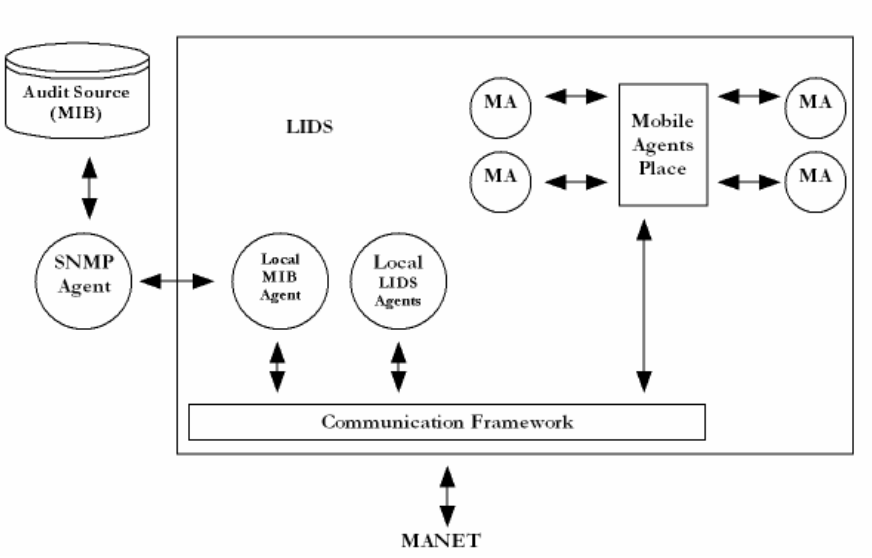

FIGURE 2: LIDS Architecture in a Mobile Node

Kachirski and Guha [45] proposed a multi-sensor intrusion detection system based on mobile agent technology. The system can be divided into three main modules, each of which represents a mobile agent with certain functionality, i.e.: monitoring, decision-making and initiating a response.

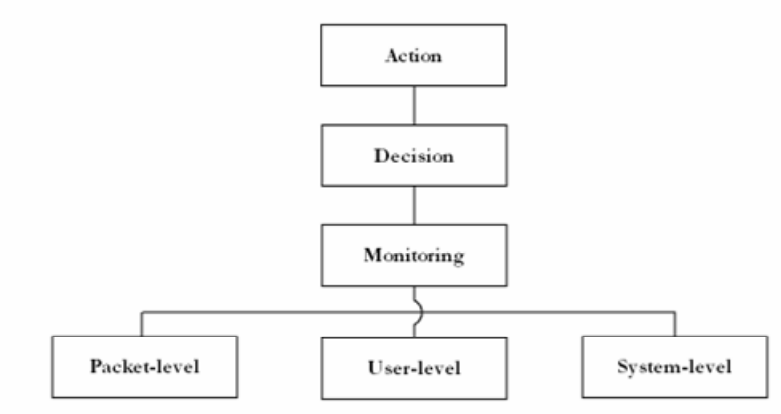

FIGURE 3: Layered Mobile Agent Architecture

- Monitoring agent: Two functions are carried out at this class of agent: network monitoring and host monitoring.

- Action agent: Every node also hosts this action agent. The action agent can initiate a response, such as terminating the process or blocking the node from the network, if it meets intrusion activities where it lives.

- Decision agent: The decision agent is run only on certain nodes, mostly at the nodes that run network monitoring agents. If the local detection agent cannot make a decision on its own due to insufficient evidence of an intrusion, it will report to this decision agent in order to investigate deeply on the suspected node

Since nodes move arbitrarily across the network, a static hierarchy is not suitable for such dynamic network topology.

Sterne et al. [46] proposed a dynamic intrusion detection hierarchy that is potentially scalable to large networks use clustering. This method is similar with Kachirski and Guha [45], but it can be structured in more than two levels. Thus, nodes on first level are cluster heads, while nodes on the second level are *leaf nodes*. In this model, every node has the task to monitor, log, analyze, respond, and alert or report to cluster heads. The Cluster heads, in addition, must also perform: 1) Data fusion/integration and data filtering, 2) Computations of intrusion, and 3) Security Management.

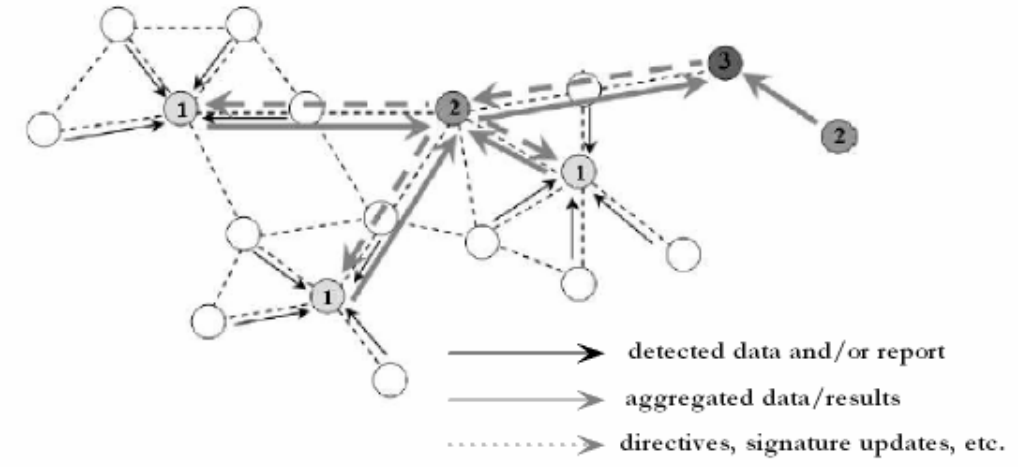

FIGURE 4: Dynamic Intrusion Detection Hierarchy

B.Sun [47] proposed Zone Based IDS (ZBIDS). In the system, the MANET is spitted into non-overlapping zones (zone A to zone I). The nodes can be categorized into two types: the intra-zone node and the inter-zone node (or a gateway node). Each node has an IDS agent run on it. This agent is similar to the IDS agent proposed by Zhang and Lee. Others components on the system are data collection module and detection engine, local aggregation and correlation (LACE) and global aggregation and correlation (GACE). The data collection and the detection engine are responsible for collecting local audit data (for instance, system call activities, and system log files) and analyzing collected data for any sign of intrusion respectively. The remainder, LACE module is responsible for combining the results of these local detection engines and generating alerts if any abnormal behavior is detected. These alerts are broadcasted to other nodes within the same zone. However, for the GACE, its functionality depends on the type of the node. If the node is an intra-zone node, it only sends the generated alerts to the inter-zone nodes. Thus, if the node is an inter-zone node, it receives alerts from other intra-zone nodes, aggregates and correlates those alerts with its own alerts, and then generates alarms. The intrusion response module is responsible for handling the alarms generated from the GACE.

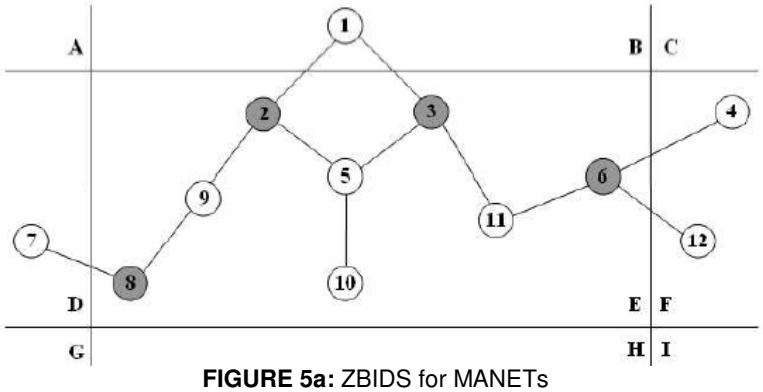

FIGURE 5a: ZBIDS for MANETs

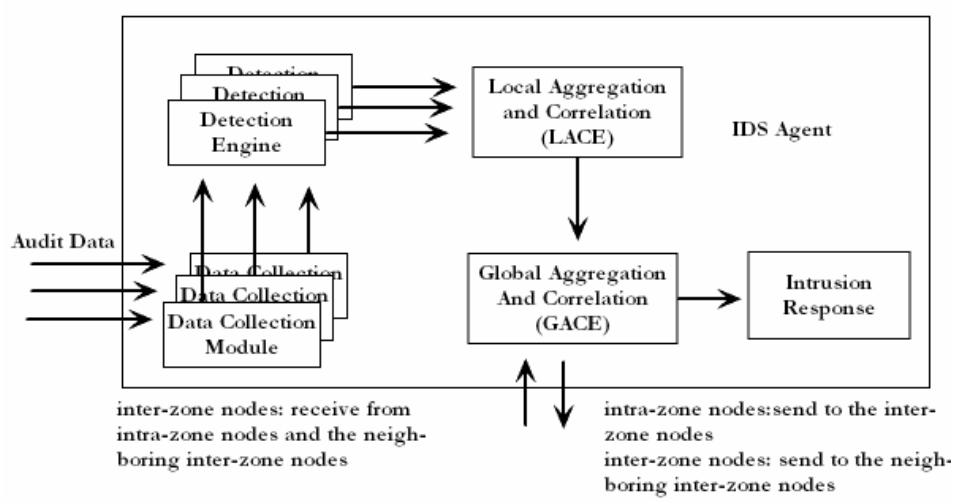

FIGURE 5b: An IDS agent in ZBIDS

4. DISCUSSION AND SUMMARY

The classification among the proposed IDS of MANET can be composed using the parameters discussed in the previous sections, i.e.: *architecture, attacks,* and *IDS detection techniques*. Most the MANET IDSes tend to have the distributed architectures and their variants. The IDS architecture may depend on the network infrastructure (see section 3.2). But the most important thing is the reasons the architecture to be configured in distributed manner. As the nature of MANET is so open, attacks source can be generated from any nodes within the MANET itself or nodes of neighboring networks. Unfortunately, this network lacks in central administration. It is difficult for implementing firewall or the IDS on the strategic points. Moreover, each node can work as client, server or router. Delivery packets need collaboration work among the nodes participant network. For these reasons, the IDS of MANET should have characteristics that follow these natures, *distributed and collaborative*. Zhang [30], Albers [44], and Sun [47] follow this idea. Meanwhile, Kachirski [45] and Sterne [46] use the variant of the distributed and collaborative. Advantage using distributed architecture is the security accident can be detected earlier. However, this architecture needs huge resources, which is difficult to be implemented in small wireless device as PDA.

All attacks type of wired networks is possible in MANET. MANET has also several typical of attacks, which are not available in the traditional wired network, such as selfish attack, black hole attack, sleep deprivation attack and others type of attacks (see section 3.1). These attacks occur because of MANET has vulnerable in the *use of wireless link, auto-configuration mechanisms, and its routing protocol*. The existing MANET IDSes have various methods to detect and to response regarding these attacks. Zhang [30] and Sun [47] proposed the IDSes which were designed for detecting the intrusion activities on the routing protocol of MANET. Albers [44] tried to extend the traditional IDS on MANET to detect incoming telnet connections and reacted if they originated from outside community's network. Sterne [46] presented a cooperative and distributed IDS that covered conventional attacks. Table 1 shows the summary of the classification of these MANET IDS.

Author(s)	Name Specific	Architecture	Addressed Attacks type			Data Source	Technique detection	Routing protocol	Environments	Contribution
			Au-then-tica-tion	Routing (black hole, etc)	Sel-fish					
Zhang and Lee, Y. Huang [30], [24]	None	Distributed and collaborative	No	Yes (misrouting, packet dropping)	No	Audit trail (event log processing)	Anomaly	AODV, DSR, DSDV	Simulation	IDS agent for collaboration detection
P. Albers, O. Camp [44]	LIDS	Distributed and collaborative	No	No	No	Audit trail (event log processing)	Misuse, anomaly	Not identified	Simulation	Local IDS mobile agent for intrusion detection model
Kachirski and Guha [45]	None	Hierarchical architecture	No	No	No	Audit trail (event log processing)	Anomaly	Not identified	Simulation	Hierarchical IDS using mobile agent
Sterne et al. [46]	None	Hierarchical architecture	No	No	No	Audit trail (event log processing)	Misuse, Anomaly	Not identified	Simulation	Dynamic intrusion detection hierarchy model
B. Sun, K.Wu, and U. W. Pooch [47]	ZBIDS	Distributed and collaborative	No	Yes (Disruption attacks)	No	Audit trail (event log processing)	Anomaly	DSR	Simulation	Routing protocol protection from disruption

TABLE 1: Comparison researches achievement on the MANET IDS.

5. CONSLUSION & FUTURE WORK

With the nature of mobile ad hoc networks, almost all of the intrusion detection systems (IDSs) are structured to be distributed and have a cooperative architecture (see table 1). Refer to the table 1, mostly the proposed research prefers using anomaly detection approach. An intrusion detection system aims to detect attacks on mobile nodes or intrusions into the networks. However, attackers may try to attack the IDS system itself. Accordingly, the study of the defense to such attacks should be explored as well.

6. ACKNOLEDGEMENTS

Authors would like to thank to the Ministry of Science, Technology and Innovation of Malaysia (the MOSTI) and Research Management Centre of UTM (RMC-UTM) – This work has been sponsored by the e-science Fund, Vot number 79027.

7. REFERENCES

1. D.B. Johnson, D.A. Maltz, et.al. *"The dynamic Source Routing Protocol for Mobile Ad hoc Networks (DSR)"*. Internet Draft, draft-ietf-manet-dsr-07.txt, work in progress, 2002

2. T. Clausen, P. Jaquet, et.al. *"Optimized link state routing protocol"*. Internet Draft, draft-ietf-manet-olsr-06.txt, work in progress, 2001

3. C.E. Perkins, P. Bhagwat. *"Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers"*. SIGCOMM 94 Conference on Communications Architectures, Protocols and Applications, 1994

4. C.E Perkins, E. Belding-Royer. "*Ad hoc On-demand Distance Vector (AODV)"*, Request For Comments (RFC) 3561, 2003

5. C. Endorf, E. Schultz and J. Mellander, *"Intrusion Detection & Prevention"*, McGraw-Hill, ISBN: 0072229543 (2004)

6. J. P. Anderson. *"Computer Security Threat Monitoring and Surveillance"*. Technical Report, James P. Anderson Co., Fort Washington, PA, 1980

7. D.E. Denning, *"An Intrusion-Detection Model"*. IEEE Transactions on Software Engineering, pp. 222- 231, 1987

8. L. Heberlein, G. Dias, et.al. *"A network security monitor"*. In Proceedings of the IEEE Symposium on Security and Privacy, pp. 296-304, 1990

9. A. Hijazi and N. Nasser. *"Using Mobile Agents for Intrusion Detection in Wireless Ad Hoc Networks"*. In Wireless and Optical Communications Networks (WOCN), 2005

10. T. F. Lunt, R. Jagannathan, et al. *"IDES: The Enhanced Prototype C a Realtime Intrusion-Detection Expert System"*. Technical Report SRI-CSL-88-12, SRI International, Menlo Park, CA, 1988

11. M. Esposito, C. Mazzariello, et.al. *"Evaluating Pattern Recognition Techniques in Intrusion Detection Systems"*. The 7th International Workshop on Pattern Recognition in Information Systems, pp. 144-153, 2005

12. S. Kumar and E. Spafford, "*A Pattern Matching Model for Misuse Intrusion Detection"*. The 17th National Computer Security Conference, pp. 11-21, 1994

13. P.A. Porras and R. Kemmerer, *"Penetration State Transition Analysis C a Rule-Based Intrusion Detection Approach"*. The 8th Annual Computer Security Application Conference, pp. 220-229, 1992

14. P. Porras and A. Valdes, *"Live Traffic Analysis of TCP/IP Gateways"*. ISOC Symposium on Network and Distributed System Security, San Diego, CA, 1998

15. H. Debar, M. Becker and D. Siboni. *"A Neural Network Component for an Intrusion Detection System"*. Proceedings of IEEE Symposium on Research in Security and Privacy, Oakland, CA, pp. 240-250, 1992

16. S. Forrest, S.A. Hofmeyr, and A. Somayaji. *"Computer Immunology"*. Communications of the ACM, pp. 88-96, 1997

17. N. Ye, X. Li, et.al. *"Probabilistic Techniques for Intrusion Detection Based on Computer Audit Data"*. IEEE Transactions on Systems, Man, and Cybernetics, pp. 266-274, 2001

18. W. Lee, S.J. Stolfo, K.W. Mok. *"A Data Mining Framework for Building Intrusion Detection Models"*. IEEE Symposium on Security and Privacy (Oakland, California), 1999

19. G. Florez, S.M. Bridges, and R.B. Vaughn, *"An Improved Algorithm for Fuzzy Data Mining for Intrusion Detection"*. The North American Fuzzy Information Processing Society Conference, New Orleans, LA, 2002

20. H. Debar, M. Dacier, and A.Wespi, *"A Revised Taxonomy for Intrusion-Detection Systems"*. Annales des Telecommunications, pp. 361-378, 2000

21. A.J. Menezes, S.A. Vanstone, P.C. Van Oorschot, *"Handbook of Applied Cryptography".* CRC Press, Inc., USA (2001)

22. A. Mishra, K. Nadkarni, and A. Patcha. *"Intrusion Detection in Wireless Ad Hoc Networks".* IEEE Wireless Communications, Vol. 11, Issue 1, pp. 48-60, 2004

23. L. Zhou and Z. J. Haas. *"Securing ad hoc networks"*. IEEE Network Magazine , 1999

24. Y. Zhang, W. Lee, and Y. Huang. *"Intrusion Detection Techniques for Mobile Wireless Networks".* Wireless Networks Journal (ACM WINET), 9(5): 545-556, 2003.

25. E.C.H. Ngai, M.R. Lyu, R.T. Chin. *"An authentication service against dishonest users in mobile ad hoc networks"*, IEEE Proceedings on Aerospace Conference, vol. 2, pp. 1275–1285 2004.

26. L. Blazevic et al. *"Self-organization in mobile ad-hoc networks: the approach of terminodes"*, IEEE Communications Magazine , pp. 166–173, 2001

27. W. Zhang, R. Rao, et. al. *"Secure routing in ad hoc networks and a related intrusion detection problem"*, IEEE Military Communications Conference (MILCOM), vol. 2, 13–16 p. 735– 740, 2003

28. J. Kong et al. *"Adaptive security for multi-layer ad-hoc networks"*. Special Issue of Wireless Communications and Mobile Computing, John Wiley Inter Science Press (2002)

29. P. Kyasanur, N. Vaidya. *"Detection and handling of MAC layer misbehavior in wireless networks"*. International Conference on Dependable Systems and Networks. pp. 173–182, 2003

30. Y. Zhang, W. Lee, *"Intrusion detection in wireless ad-hoc networks"*, The 6th Annual International Conference on Mobile Computing and Networking, pp. 275–283, 2000

31. Y. Hu, A. Perrig, and D. Johnson. *"Packet leashes: A defense against wormhole attacks in wireless ad hoc networks"*. In Proceedings of IEEE INFOCOM'03, 2003

32. Y. Hu, A. Perrig, D. Johnson, *"Ariadne: a secure on-demand routing protocol for ad hoc networks".* ACM MOBICOM, 2002

33. Y. Hu, A. Perrig, and D. Johnson. *"Rushing attacks and defense in wireless ad hoc network routing protocols"*. In Proceedings of ACM MobiCom Workshop - WiSe'03, 2003

34. J. R. Douceur. *"The sybil attack"*. The 1st International Workshop on Peer-to-Peer Systems pp. 251–260, 2002.

35. J. Hubaux, L. Buttya´n, S. Capkun, "*The quest for security in mobile ad hoc networks."* The 2nd ACM International Symposium on Mobile Ad Hoc Networking and Computing, 2001

36. P. Papadimitratos, Z.J. Haas, E.G. Sirer, *"Path set selection in mobile ad hoc networks"*, The Proceedings of the 3rd ACM International Symposium on Mobile Ad Hoc Networking and Computing, pp. 1–11, 2002

37. B. DeCleene et al. *"Secure group communications for wireless networks".* IEEE Military Communications Conference, 2001.

38. S. Bo, W. Kui, U.W. Pooch. *"Towards adaptive intrusion detection in mobile ad hoc networks".* IEEE Global Telecommunications Conference, pp. 3551–3555, 2004

39. C. Douligeris, A. Mitrokosta, *"DDoS attacks and defense mechanisms: classification and state-of-the-art".* Computer Networks: The International Journal of Computer and Telecommunications Networking 44 (5):643–666, 2004

40. C.M. Chlamtac, J.J.-N. Liu, *"Mobile ad hoc networking: imperatives and challenges"*, Ad Hoc Networks 1, 2003

41. H. Yang, H.Y. Luo, et.al. *"Security in Mobile Ad Hoc networks: challenges and solutions".* IEEE Wireless Communications, pp.38–47, 2004.

42. C. Krugel and T. Toth. *"Applying mobile agent technology to intrusion detection".* In ICSE Workshop on Software Engineering and Mobility, 2001.

43. T. Anantvalee and J. Wu. *"A Survey on Intrusion Detection in Mobile Ad Hoc Networks"*, Book Series Wireless Network Security, Springer, pp. 170 – 196, ISBN: 978-0-387-28040-0 (2007)

44. P. Albers, O. Camp, et al. *"Security in Ad Hoc Networks: a General Intrusion Detection Architecture Enhancing Trust Based Approaches".* Proceedings of the 1st International Workshop on Wireless Information Systems (WIS-2002), pp. 1-12, April 2002

45. O. Kachirski, R. Guha. *"Effective Intrusion Detection Using Multiple Sensors in Wireless Ad Hoc Networks."* Proceedings of the 36th Hawaii International Conference on System Sciences (HICSS'03), IEEE, 2003

46. D. Sterne, P. Balasubramanyam, et al. *"A General Cooperative Intrusion Detection Architecture for MANETs"*. In Proceedings of the 3rd IEEE International Workshop on Information Assurance (IWIA'05), pp. 57-70, 2005

47. B. Sun, K.Wu, and U. W. Pooch. "*Alert Aggregation in Mobile Ad Hoc Networks"*. The 2003 ACM Workshop on Wireless Security in conjuction with the 9th Annual International Conference on Mobile Computing and Networking (MobiCom'03), pp. 69-78, 2003

48. C. Ko, J. Rowe, P. Brutch, K. Levitt, *"System Health and Intrusion Monitoring Using a hierarchy of Constraints".* In Proceedings of 4th International Symposium, RAID, 2001