Investigating Intrusion Detection Systems in MANET and Comparing IDSs for Detecting Misbehaving Nodes

Marjan Kuchaki Rafsanjani, Ali Movaghar, and Faroukh Koroupi

***Abstract*—**As mobile ad hoc networks (MANET) have different characteristics from wired networks and even from standard wireless networks, there are new challenges related to security issues that need to be addressed. Due to its unique features such as open nature, lack of infrastructure and central management, node mobility and change of dynamic topology, prevention methods from attacks on them are not enough. Therefore intrusion detection is one of the possible ways in recognizing a possible attack before the system could be penetrated. All in all, techniques for intrusion detection in old wireless networks are not suitable for MANET. In this paper, we classify the architecture for Intrusion detection systems that have so far been introduced for MANETs, and then existing intrusion detection techniques in MANET presented and compared. We then indicate important future research directions.

***Keywords*—**Intrusion Detection System(IDS), Misbehaving nodes, Mobile Ad Hoc Network(MANET), Security.

I. Introduction

A mobile ad hoc network (MANET) is relatively new communication paradigm. MANET does not require expensive base stations of wired infrastructure. Nodes within radio range of each other can communicate directly over wireless links, and those that are far apart use other nodes as relays. Each host in a MANET also acts as a router and routers are mostly multi hop [1]. MANET is self-organized in such a way that a collection of mobile nodes without a fixed infrastructure and central management is formed automatically. Each node is equipped with a wireless transmitter and receiver that communicate with other nodes in the vicinity of its radio communication range. If a node decides to send a packet to a node that is outside its radio range, it requires the help of other nodes in the network. Due to the fact that mobile nodes are dynamic and they constantly move in and out of their network vicinity, the topologies constantly change.

Initially, MANET was designed for military applications, but, in recent years, has found new usage. For example, search and rescue mission, data collection, virtual classes and conferences where laptops, PDA or other mobile devices are in wireless communication. Since MANET is being used widespread, security has become a very important issue. The majority of routing protocols that have been proposed for MANET assumes that each node in the network is a peer and not a malicious node. Therefore, only a node that compromises with an attacking node can cause the network to fail.

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) [2][3].

In this paper, IDS architectures in MANET have been classified so that each one is suitable for different network infrastructures. Then different techniques for intrusion detection regarding nodes cooperation will be investigated and compared.

II. IDS Architectures in Manet

The network architectures for MANET with regards to its applications are either flat or multi layer. 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 [4].

A. Stand-alone IDSs

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

M. Kuchaki Rafsanjani is with Islamic Azad University, Science and Research Branch, Tehran, Iran (corresponding author to provide phone: +989131911246; e-mail: kuchaki.m@srbiau.ac.ir).

A. Movaghar is with the Department of Computer Engineering, Sharif University of Technology, Tehran, Iran (e-mail: movaghar@sharif.edu).

F. Koroupi is with Islamic Azad University, Baft Branch, Baft, Iran (e-mail: Koroupi@iauk.ac.ir).

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 multi layered network infrastructure. Due to the fact that exclusive node information is not enough to detect intrusions, thus this architecture has not selected in many of the IDS for MANETs [3].

B. Distributed and Cooperative IDSs

MANETs are distributed by nature and requires nodes cooperation. Zhang and Lee [5] 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 neighboring IDS agents cooperate with each other when there is not any convincing evidence in global intrusion detection. This architecture, which is similar to stand-alone IDS architecture, is more suitable for flat network infrastructure compared with multi-level infrastructure.

C. Hierarchical IDSs

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 [3].

D. Mobile Agent for IDSs

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 [6]. 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.

III. 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 in the active attacks, operations such as repetition, changing, or deletion of data are necessitated. Certain nodes in MANETS can produce attacks which cause congestion, distribution of incorrect routing information, services preventing proper operation, or disable them [7].

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 [8],[9]. 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 "blackhole" attack [10],[11].

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 [12],[13].

Selfish nodes can intensively lower the efficiency of the network since they do not easily participate in the network operations. 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 [11], [14],[15],[16].

If a node participated in routes finding but does not forward a packet, it is a misleading node and misleads other nodes. But if a node does not participate in routes finding, it is a selfish node [3].

IV. 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 Giuli and Baker [17] performed show that only a few misbehaving nodes can reduce entire system efficiency. A few techniques and protocols detecting and confronting misbehaving nodes are available [18],[19].

Many intrusion detection systems have been proposed and most of them are tightly related to routing protocols.

A. Watchdag and Pathrater

These two techniques were presented by Marti, Giuli and Baker [17] and were added to the standard routing protocol in ad hoc networks. The standard is Dynamic Source Routing protocol DSR [20]. 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. Fig. 1 shows how the Watchdog technique operates.

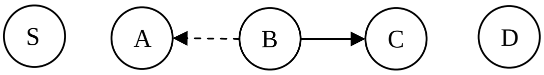

Fig. 1 Watchdog operation

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 behaviors.

B. CONFIDANT

Bachrgger and Leboudec [18] 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 behavior of all its neighboring 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).

C. CORE

Michiardi and Molva [19] 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 decreased. In contrast, a positive rating is given to a node when a positive report is received from this node and its reputation increases.

D. OCEAN

Bansal and Baker [20] 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

TABEL I
INTRUSION DETECTION TECHNIQUES COMPARISON

ID Techniques		Watchdog/ Pathrater	CONFIDANT	CORE	ExWatchdag	OCEAN	Cooperative IDS
Observation	self to neighbor	yes	yes	yes	yes	yes	yes
	neighbor to neighbor	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		yes	yes	no	yes	yes	n/a
Architecture		Distributed and cooperative				Stand alone	Hierarchical

false accusation from second-hand reputation exchanges, therefore OCEAN can be viewed as a stand-alone architecture.

OCEAN divides routing misbehavior 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. In order to discover misleading routing behaviors, after a node forwards a packet to its neighbor, it saves the packet and if the neighboring 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 neighboring node. If the rating is lower than faulty threshold, neighboring 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.

E. *Cooperative Intrusion Detection System*

Huang and Lee [21] proposed a cluster-based cooperative intrusion detection system, which is similar to Kachirski and Guha's system [22]. In this method, an IDS not only is 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 [23]. 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 [3].

F. *ExWatchdog IDS*

Nasser and Chen [24] 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 [25]. Watchdog resides in each node and is based on overhearing. Through overhearing, each node can detect the malicious action of its neighbors 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.

V. INTRUSION DETECTION TECHNIQUES COMPARISION FOR DETECTING MISBAHAVING 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 wrongly accusations. When each node has a different transfer range or implements directional antennas, the Watchdog can not monitor the neighboring nodes accurately. All IDSs discussed so far can identify selfish nodes. CORE can not detect malicious nodes misbehaviors, but others can detect some of them such as unusually frequent rout update, header change, or payload of packets, etc. Table I represents the final comparison among discussed IDSs.

VI. FUTURE RESEARCH DIRECTIONS

In general, 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 [16][26].

Sometimes the attackers may try to attack the IDS system itself. Therefore, defense against such attacks should be considered further.

VII. Conclusion

Ad hoc networks are an increasingly promising area of 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.

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 damage is caused in system or data. The aim of an intrusion detection system is detecting attacks on mobile nodes or intrusions into network. Intrusion detection systems, if well designed, effectively can identify misbehaving activities and help to offer adequate protection. Therefore, an IDS has become an indispensable component to provide defense-in-depth security mechanisms for MANETs.

References

[1] B. Sun and L. Osborne Young, “Intrusion detection techniques in mobile ad hoc and wireless sensor networks,” *IEEE Wireless Communications*, pp. 56–63. October 2007.

[2] L. Zhou, Z.J. Haas, “Securing ad hoc networks”, *IEEE Network Magazine Special Issue on Network Security*, vol. 13, no. 6, pp. 24-30, Nov/Dec 1999.

[3] Y. Xiao, X. Shen, and D.Z. Du, *Wireless/Mobile Network Security*, Springer, 2006. Ch.7.

[4] P. Brutch and C. Ko, “Challenges in intrusion detection for wireless ad-hoc networks,” in *Proc. 2003 Symposium on Applications and the Internet Workshop*, January 2003, pp. 368-373.

[5] Y. Zhang, W. Lee, and Y. Huang, “Intrusion detection techniques for mobile wireless networks,” *Wireless Networks Journal (ACM WINET)*, vol. 9, no. 5, pp. 545-556, September 2003.

[6] A. Mishra, K. Nadkarni, and A. Patcha, “Intrusion detection in wireless ad hoc networks,” *IEEE Wireless Communications*, vol. 11, pp. 48-60, February 2004.

[7] A. Karygiannis, E. Antonakakis, and A. Apostolopoulos, “Detecting critical nodes for MANET intrusion detection systems,” in *Proc. 2nd International Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing*, 2006.

[8] J. Kong, *Adaptive Security for Multi-layer Ad Hoc Networks*, Special Issue of Wireless Communications and Mobile Computing, John Wiley InterScience Press, 2002.

[9] L. Blazevic, L. Buttyan, S. Capkun, S. Giordano, J. Hubaux, and J. Le Boudec, “Self-organization in mobile ad-hoc networks: the approach of terminodes,” *IEEE Communications Magazine*, vol. 39, no. 6, pp. 166–174, 2001.

[10] Y. Zhang, and W. Lee, “Intrusion detection in wireless ad-hoc networks,” in *Proc. 6th Annual International Conference on Mobile Computing and Networking*, Boston, MA, USA, 2000, pp. 275–283.

[11] N. Komninos, D. Vergados, and C. Douligeris, “Detecting unauthorized and compromised nodes in mobile ad hoc networks,” *Elsevier Ad hoc network*, vol. 5, no. 3, pp. 289-298, 2007.

[12] P. Kyasanur, and N. Vaidya, “Detection and handling of MAC layer misbehavior in wireless networks,” Int. *Conf. on Dependable Systems and Networks (DSN’03)*, 2003, pp. 173–182.

[13] Y. Hu, A. Perrig, and D. B. Johnson, “Packet leashes: A defense against wormhole attacks in wireless networks,” in *Proc. 22th Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM’03)*, Pittsburgh, PA, USA, vol. 3, 2003, pp. 1976-1986.

[14] P. Papadimitratos, Z.J. Haas, and E.G. Sirer, “Path set selection in mobile ad hoc networks,” in *Proc. 3rd ACM International Symposium on Mobile Ad Hoc Networking and Computing*, Lausanne, Switzerland, 2002, pp. 1–11.

[15] B. Sun, W. Kui, and U.W. Pooch, “Towards adaptive intrusion detection in mobile ad hoc networks,” in *Proc. IEEE Global Telecommunications Conference (GLOBECOM’04)*, Beaumont, TX, USA, vol. 6, 2004, pp. 3551–3555.

[16] M. K. Rafsanjani, A. Movaghar, “Identifying monitoring nodes in MANET by detecting unauthorized and malicious nodes,” in *Proc. 3rd IEEE Int. Symposium on Information Technology (ITSIM’08)*, August 2008, pp. 2798-2804.

[17] S. Marti, T.J. Giuli, K. Lai, and M. Baker. “Mitigating routing misbehavior in mobile ad hoc networks,” in *Proc. 6th Annual Int. Conf. on Mobile Computing and Networking (MobiCom'00)*, Boston, MA, August 2000, pp.255-265.

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

[19] P. Michiardi and R. Molva, “Core: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks,” *Communication and Multimedia Security Conference (CMS'02)*, September 2002.

[20] S. Bansal and M. Baker, “Observation-based cooperation enforcement in ad hoc networks,” *Research Report cs.NI/0307012*, Stanford University, 2003.

[21] Y. Huang and W. Lee, “A cooperative intrusion detection system for ad hoc networks,” in *Proc. ACM Workshop on Security in Ad Hoc and Sensor Networks (SASN'03)*, October 2003, pp. 135-147.

[22] O. Kachirski and R. Guha, “Effective intrusion detection using multi-ple sensors in wireless ad hoc networks,” in *Proc. 36th Annual Hawaii Int. Conf. on System Sciences (HICSS'03)*, January 2003, p. 57.1.

[23] Y. Huang, W. Fan, W. Lee, and P. Yu, “Cross-feature analysis for detecting ad-hoc routing anomalies,” in *Proc. 23rd IEEE Int. Conf. on Distributed Computing Systems (ICDCS'03)*, May 2003, pp. 478-487.

[24] N. Nasser and Y. Chen, “Enhanced intrusion detection system for discovering malicious nodes in mobile ad hoc network,” in *Proc. IEEE Int. Conf. on Communication (ICC’07)*, June 2007, pp. 1154-1159.

[25] A. Hasswa, M. Zulker, and H. Hassanein, “Routeguard*: an intrusion* detection and response system for mobile ad hoc networks,” *Wireless and Mobile Computing, Networking and Communication*, vol. 3, August 2005, P336-343.

[26] M. K. Rafsanjani, A. Movaghar, “Identifying monitoring nodes with selection of Authorized nodes in mobile ad hoc networks,” *World Applied Sciences Journal*, vol. 4, no.3, pp. 444-449, 2008.