Guidelines on Selecting Intrusion Detection Methods in MANET

Yi Li and June Wei
University of West Florida
Pensacola, Florida 32514, USA

Abstract

Applications of Mobile Ad Hoc Networks (MANET) are increasing in practice; however, MANET is venerable to attacks due to its mobile and ad hoc natures. The security issue is becoming a major concern and bottle neck in the applications of MANET; therefore, selections of intrusion detection methods are especially important for MANET applications. In the current paper, an overview of existing IDS for MANET is conducted based on reviewing features, security issues and requirements of MANET for intrusion detection systems (ISD). A comparison study is conducted to compare existing intrusion detection methods based on inputs, outputs, processes, advantages and disadvantages. Some guidelines are also proposed in selecting intrusion detection methods. The results of the current research are useful for educational and industrial professionals who are interested in information systems security in the wireless world. This paper also presents a case study of a MIS/CIS/CS curriculum on the first introduction of the new technology for IDS in MANET.

Keywords: Mobile ad hoc network, MANET, intrusion detection system, IDS, wireless network

1. INTRODUCTIONS

Next generation wireless network will include infrastructure-d wireless networks and infrastructure-less mobile ad hoc networks (MANET). MANET will have significant application in the coming years, both as large-area mobile multi-hop wireless and personal area network, including mobile commerce.

Mobile Commerce uses wireless device and data connection to result in the transfer of values in exchange of information, services or goods (Wei 2004; Andreou 2002). Mobile commerce has huge potential markets. The industry researcher GartnerGroup predicted that by 2005, e-commerce transactions conducted in mobile channel will reach up to $1.8 trillion by 2005 (May, 2001; Gartner 2000).

MANET may bring a revolution to the business model of mobile commerce if MANET is used as the underlying network technology for mobile commerce. The ad hoc nature of MANET makes new mobile commerce models different from the present mobile commerce models which using mobile phone network, one type of the infrastructure-d wireless network and the major underlying network technology.

One major challenge to the wide application of mobile commerce is the security (Wei, 2003). Mobile commerce will remain in a niche market for a few years until the security issue is properly addressed (Gillick and Vanderhoof, 2000). Security for MANET is very important for MANET applications in mobile commerce. Among all security measurements for MANET, intrusion detection is a crucial issue because MANET relies much more on intrusion detection for security than wired network.

Mishira (Mishra and Nadkarni, 2004) and Brutch (Brutch and Ko, 2003) conducted two surveys in intrusion detection for MANET. Both surveys focus on the discussion of the current state of the research in IDS of

MANET, and analyzed and compared the proposed IDS in the current literatures.

The current research is the first attempt to propose a framework for comparison study for IDS in MANET, and to analyze the proposed IDS by decomposing them into different components or modules, such as communication and decision making mechanism. Moreover, a number of guidelines in selecting the different intrusion detection methods in developing IDS for MANET are also the first attempt. These guidelines are based on the requirement and resources of the target network.

The current paper focuses on the infrastructure-less MANET and is organized as follows: Section 2 presents an overview of existing intrusion detection systems (IDS) for MANET is conducted based on reviewing features, security issues and requirements of MANET for ISD. Section 3 develops a comparison study framework and presents comparison study on IDS in MANET based inputs, outputs, process methods, advantages and disadvantages. Section 4 develops guidelines on how to select intrusion detections methods for MANET. Section 5 provides conclusions.

2. Literature Review

2.1 MANET

MANET is an IP based network consisting of a number of wireless and mobile machine nodes linked with radio. In operation, these nodes do not depend on any predefined infrastructure or centralized administration. Such network can be used in a conference or classroom, even in battlefields. In MANET, nodes within the radio range communicate with each other directly via wireless links, while nodes out of the radio range need an intermediate node to forward their messages. Each node can act both as a router as well as a host.

The characteristics of MANET are identified as follows (Rafique, 2002; Albers and Camp, 2003; Smith, 2001):

- Autonomous terminal: Each node in MANET is autonomous and is both router and host.
- Distributed: MANET is distributed in its operation and functionalities, such as routing, host configuration and security. For instance, unlike wired network, MANET can not have a centralized firewall (Albers and Camp, 2003).
- Multi-hop routing: If the source and destination of a message is out of the radio range of one node, a multi-hop routing is necessary.
- Dynamic network topology: Nodes are mobile and can join or leave the network at any time; therefore, the topology is dynamic.
- Fluctuating link bandwidth: The stability, capacity and reliability of wireless link is always inferior to wired links.
- Thin terminal: The mobile nodes are often light weight, with less powerful CPU, memory and power.
- Spontaneous and mobile: minimum intervention is needed in configuration of the network. The routing protocol should be an adapted one that allows users to communicate in the network. It should also support security.

Some existing security technologies for wired network, such as encryption, can be utilized in MANET. However, because of the mobile and ad hoc nature of MANET, the applications of MANET, are limited. Other technologies, such as firewall, do not apply to MANET, because of the lack of a centralized authority.

Same as the wired network, MANET faces the security threat such as passive eavesdropping, spoofing, and denial of service. At the same time, because of its ad hoc nature, it suffers from more security threats. Threats to MANET can be classified into two groups:

- Vulnerabilities accentuated by the ad hoc nature: The topology of MANET is mainly determined by geographical locations and by radio range of the nodes. Therefore, it does not have a clearly defined physical boundary. In wired network, a centralized firewall can implement the access-control. However, in MANET, access-control can not be

done with a centralized firewall (Albers and Camp, 2003). Other attacks, such as denial of service (DOS) still threat MANET, even worse than for wired network, since the routing and auto configuration framework of MANET are more venerable to such attack.

- Vulnerabilities specific to the ad hoc nature: The routing and auto configuration mechanism of MANET introduces opportunity for more attack because in both mechanisms, all nodes have full trust between each other (Albers and Camp, 2003).

In wireless-network, the decision making in many important protocols, such as routing, is collaborative. Attack can be designed to make use of the collaborative nature of the algorithm and cause the system to break down. For instance, the MAC layer protocol in wireless network is much more venerable than that in fixed network. The nodes collaborate with each other to determine who has the communication channel for transmission and how to render the channel by following in predefined protocol. If one node is compromised and acts maliciously, the protocol will not work and the network will break down, resulting into Denial of Service. In wired network, it rarely happens because the MAC layer is isolated from the outside with layer-3 devices such as firewall or gateway (Zhang and Lee, 2003).

The auto configuration also introduces vulnerabilities. The configuration mechanism uses information given by the nodes to calculate IP address and to determine whether IP address is already in use. Then a malicious node can pretend to use the IP address of an incoming node. This blocks the incoming node from joining the network.

The MANET nodes usually use battery power. An attacker can make a node to exhaust its power just by forcing it to forward packets. This is called "sleep deprivation torture" (Albers and Camp, 2003).

In wireless network, when an outside entity connect to the network, it does not need physical connection nor to pass some security defense lines such as firewall or gateway, therefore, wireless network's nature make itself more venerable to attacks. Attacks can come from any place and can target at any node inside the wireless network. In other words, in wireless network, the defense line is very vague and each node has a risk of being compromised (Zhang and Lee, 2003).

The wireless network allows its nodes to roam as autonomous independent unit. Then it is very likely that a node is high jacked because of lack of physical protection, for instance, a hand-held device is stolen. Tracking mobile nodes in large scale network is very difficult. Then attack can be launched from the compromised nodes, which are more damaging and hard to detect.

The usage of intrusion prevention techniques is more limited in their effect. For instance, we can use encryption or user authentication to implement defense. However, in wireless network, it is very possible that some nodes, such as a hand held device get stolen and compromised, which rarely happens in wired network. And such nodes have private key on them. This will void the encryption defense.

The security goals of MANET include availability, integrity, authentication, confidentiality, integrity and non-repudiation. Availability means the MANET should be able to survive denial of service attacks; Denial of service can happen at any layer of the MANET (For instance, attacker can distort the routing protocol at network layer to cause the network stop); Confidentiality means the ability to protect confidential information from unauthorized user; Integrity means message should not be corrupted in transmission (The corruption could be caused by network failure or attacks); Authentication enables a node to ensure the true identity of a peer node (Without authentication, attack can perform node masquerade and gain unauthorized access to the network); and Non-repudiation ensures the sender node of a message can not deny the sending of the message. This is useful in detecting and isolating a compromised node (Rafique, 2002).

In order to overcome these vulnerabilities and achieve the security

goals, MANET needs the following security measures:

- Protecting routing mechanism: The paper already shows that MANET's routing is more likely under attack. The possible solution is to use cryptographic scheme or develop secure routing protocol.
- Protecting key management scheme: secure distribution of key is difficult in MANET. Possible solution is a scheme based on asymmetric key cryptograph.
- Intrusion detection: This is the focus of the paper and will be discussed in detail later (Rafique, 2002).

2.2 IDS in MANET

Intrusion detection system serves as an alarm mechanism for a computer system. It detects the security comprises happened to a computer system and then issues an alarm message to an entity, such as a site security officer so that the entity can take some actions against the intrusion (Axelsson, 2000;Greg, 2004).

An IDS contains an audit data collection agent, which keep track of the activities within the system, a detector which analyzes the audit data and issues an output report to the site security officer (Axelsson, 2000).

In the discussion of IDS in MANET, two concepts need to be distinguished: intrusion detection techniques and intrusion detection architecture. Intrusion detection techniques refer to the concepts such as anomaly and misuse detection. They mainly solve the problems how an IDS detects an intrusion with a certain algorithm, given some audit data as input data. It can be viewed as an algorithm. The intrusion detection architecture, however, deals with problems in a larger scope.

Intrusion detection architecture needs to employ certain intrusion detection techniques as a module. But it also contains many other modules, such as a module on how the nodes in a network can collaborate in intrusion detection decision making. In wired network, a node can usually make intrusion detection decision based on the data collected locally. Therefore, an intrusion detection technique can meet the need for intrusion detection once it is deployed on a node. In wireless network, however, it is very difficult for a node to make decision just based on data collected locally. Nodes must collaborate or exchange data at least in making an intrusion detection decision. Therefore, an architecture to define the roles of different nodes and the way they communicate is extremely important in wireless IDS.

The intrusion detection technique is basically independent from the architecture or environment. In other words, anomaly and misuse detection can be utilized in wireless environment just as they are in wired network. The difference in implementation is mainly on what audit data to take as input to the algorithm. However, most IDS in MANET utilize anomaly detection because of the special nature of MANET.

The most literature on IDS in MANET the author reviews focus on different architectures of IDS in MANET, rather than different detection techniques. Many literatures do not describe the detection techniques used in detail. Some even just states that the architecture can utilize both anomaly and misuse detection techniques. The current paper, therefore, focuses on the different architectures of IDS, rather than the detection techniques that the architectures use.

This section first discusses the attacks in MANET and the security task of IDS in MANET. Then, the requirements for IDS in MANET are identified. Finally, the possible architectures of IDS in MANET are analyzed.

2.2.1 Attacks in MANET

Attacks in MANET can be classified in terms of consequence and techniques (Lee and Huang, 2003). Based on consequence, attacks can be grouped into:

- Black hole: all packets are routed to a specific node which will not forward them at all
- Routing loops: cause a loop in routing path.
- Network partition: the network is divided into sub networks where nodes can not communicate each

other even though path exists between them.
- Selfishness: A node will not serve as a router for other nodes.
- Sleep deprivation: A node is forced to use up its battery.
- Denial of Service: A node is prohibited from sending or receiving packets (Lee and Huang, 2003; Zhou and Haas, 1999).

Based on the techniques of attack, they can be grouped into:

- Cache poisoning: information in routing tables is modified, deleted or contains false information.
- Fabricated Route Messages: route messages, such as route requests and replies with malicious information are inserted into the network. They can be done by:
  (a) False source route: a wrong route is broadcasted in the network, such as setting the route cost to 1 no matter where the destination is.
  (b) Maximum sequence: alter the sequence field in control messages to the maximum possible value. This will cause nodes to invalidate all legitimate messages with reasonable sequence filed value.
- Rushing: In several routing protocols of MANET, only the messages that arrive first is accepted by the recipient. The attacker can block legitimate messages that arrive later by distributing a false control message.
- Wormhole: A path is created between two nodes that can be used to transmit packets secretly.
- Packet dropping: A node drops packets that are supposed to be routed.
- Spoofing: insert packet or control message with false or altered source address.
- Malicious flooding: Forward unusually large amount of packets to some targeted nodes (Lee and Huang, 2003).

2.2.2 Security Tasks of IDS in MANET

Brutch and Ko (2003) presented two security tasks of IDS in MANET:

- Detect attacks against routing protocol: In MANET, attacker may inject, replay, or distort routing information in order to partition the network or cause excessive load, while inside nodes may pass incorrect routing information (Sun and Wu, 2003; Lee, 2002; and Marti, 2000).
- Detect attacks against mobile nodes: This is just like in wired network; we need to protect individual workstation.

2.2.3 Requirements for IDS in MANET

The difference between wireless and wired network as regard of IDS are as follows:

- IDS for MANET must work with localized and partial audit data. In MANET, the audit data is always localized and partial because MANET does not have a fixed infrastructure such as firewall or gateway that is used in wired network to collect complete and global audit data (Zhang and Lee, 2003).
- Network-based IDS does not work for wireless network.
- It is more difficult to IDS in MANET to distinguish between normal and intrusion traffic. In wireless network, there is often no clear line between normal/abnormal activities: In wireless network the connection is not stable and mobile nodes can join and leave the network at any time. For instance, a node which is temporarily out of synchronization may send packets that could be considered packets of attack activities. (Zhang and Lee, 2003).
- IDS should utilize minimum resources. The wireless network does not have stable connection and physical resource of network and devices, such as bandwidth and power, are limited. Disconnection

can happen at any time (Zhang and Lee, 2003). In addition, the communication between nodes for IDS purpose should not take too much bandwidth resources.

- Encryption in communication is difficult to achieve. The communication between IDS on different nodes must be secure to not allow attacks gain the access to such communication. However, encryption in Manet is a difficult task itself. In wired network, because of the requirement of physical connection for access, this problem is less obvious.
- IDS can not assume any node is secure. Unlike in a wired network, Manet nodes can be very likely compromised. Therefore, in cooperative algorithm, the IDS must not assume that any nodes can be fully trusted.
- IDS must address high false alarm rate problem. It is difficult to obtain enough audit data to make a intrusion detection decision, because the bandwidth of Manet is much restricted compared with wired network. As a result, IDS in Manet can easily result in either having too much false alarm or missing many attacks (Kong and Lou, 2002).

There are three development issues need to be addresses:

- Find an appropriate architecture of IDS that will fit the mobile and ad-hoc nature of the wireless network.
- Find a way to effectively use the audit data source in wireless network in anomaly detection. As mentioned earlier, the audit data in wireless network is often partial and local.
- Find a way to effectively distinguish attack traffic from normal traffic, especially that normal traffic that seems abnormal due to factors such as poor network connections. Otherwise, the IDS will have a high false alarm rate (Zhang and Lee, 2003).

Levente (2002) identified the requirements of IDS for MANET as follows:

- Be truly distributed, which means IDS must detect intrusion on each node, but nodes can collaborate in making decision on whether to issue an alarm.
- To deal with local and partial audit data, IDS may need to sense anomaly happened on other hops.
- To deal with the problem that no clear line between normal/abnormal, IDS need to obtain high detection rate and low false alarm.
- Given the resources constraints on wireless network, IDS should not consume too much resource, including power. Therefore, IDS should have run-time efficiency.

2.2.4 Architectures and Detection Decision Making Models for IDS in MANET

Several possible architectures of IDS in MANET existing include stand-along IDS, distributed and cooperative IDS, and hierarchical IDS.

- Stand-alone IDS: In this architecture, each host has a IDS and detect attacks independently. There is no cooperation between nodes and all decision is based on local nodes. This architecture is not effective enough but can be utilized in an environment where not all nodes are capable of running IDS (Brutch and Ko, 2003).
- Distributed and Cooperative IDS: In this architecture, each node has a IDS agent and make local detection decision. At the same time, all the nodes participate in a global detection decision making. This is more suitable to a flat MANET (Brutch and Ko, 2003).
- Hierarchical IDS: This architecture is designed for multi-layer MANET. In a multi-layered MANET, cluster-head (CH) nodes centralized routing for all nodes in the cluster and can support security measures including IDS. In addition, the CH nodes can also detect attacks against the virtual

backbone's routing protocol made by Byzantine CH nodes, which is extremely important in MANET (Brutch and Ko, 2003).

Moreover, two types decision making for intrusion detection in MANET existing include collaborative decision making and independent decision making as follows:

- Collaborative decision making: Each node participates actively in the intrusion detection process. Once one node detects an intrusion with confidence high enough, this node can start a response to the intrusion. In a simple implementation of this design, a majority voting scheme is used to determine whether attack happens (Lee and Zhang, 2000). This design can also use more complicated decision making schemes such as fuzzy logic. This design has some weak points in terms of security. It is more easily under the attacks such as denial of service and spoofed intrusion. In spoofed intrusion, a malicious node triggers full-forced intrusion response, which affects the whole network (Kachirski and Guha, 2002).
- Independent decision making: In this framework, certain nodes are assigned for intrusion detection. These nodes collect intrusion alerts from other nodes and determine whether any node in the network is under attack. These nodes do not need other nodes' participation in decision making. This design also has weak points: in order to make a good decision, the decision making node need collect a large amount of data from other nodes. However, such collection is very expensive in MANET, whose the network resources are especially limited (Kachirski and Guha, 2002).

3. COMPARISON STUDY ON IDS IN MANET

3.1 Framework on Comparison Study

Figure 1 illustrated a framework developed in the current research for the comparison study on intrusion detection in MANET. There are mainly three flows and seven components. The detailed descriptions for each of these flows and components are presented in the following.

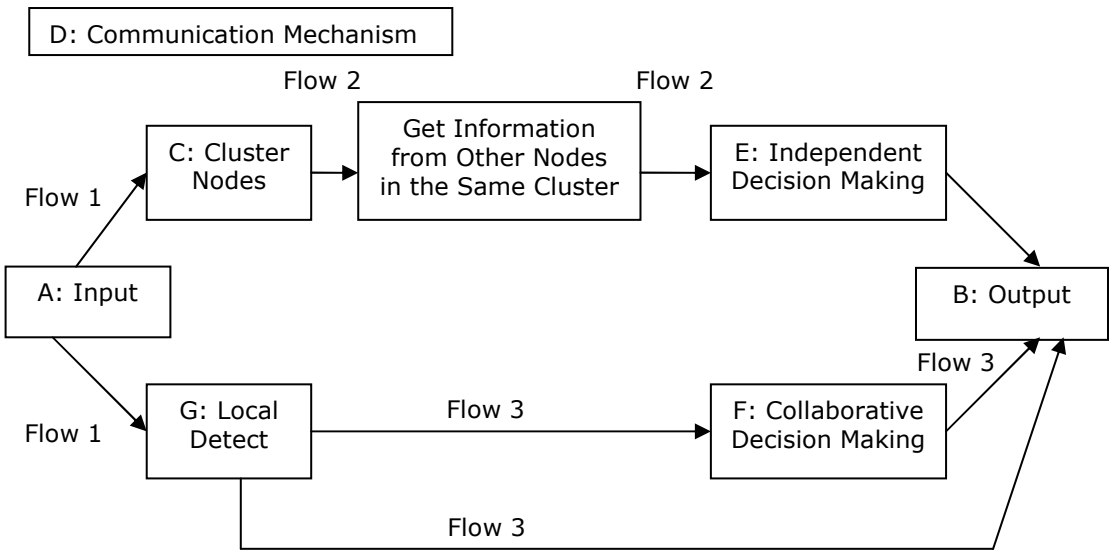

Figure 1. Framework of Comparison Study on Intrusion Detections in MANET

Input: The data to be collected by the IDS. It mainly includes system audit data, network packet or statistics of such data, for instance the statistics of updates in routing table.

Cluster nodes: certain algorithms are run on the network so that the network be partitioned into a number of clusters. A cluster usually has a node as the cluster head. The network partition and cluster head selection is dynamic.

Local detect: The IDS module or agent on a single node run intrusion detection algorithm to determine whether intrusion happens on the local node.

Get information from other nodes: This usually happens on cluster head. Because of the distributed and ad hoc nature of MANET, the local information on a single node is often insufficient for detection decision making. Therefore, the IDS need to collect information from other nodes rather than the node it resides in to make accurate detection.

Independent detection decision making: The IDS on the cluster head make intrusion decision with all the information it acquires.

Collaborative detection decision making: Several nodes participate in a collaborative decision making process, for instance a voting to make the intrusion decision. Usually, before the voting, each of the participating nodes already makes an initial decision. They need to aggregate the initial decisions to make a more accurate group decision.

Flow 1: First input is collected for IDS. Then, some IDS group network nodes into clusters or zones and other IDS do not group nodes.

Flow 2: In IDS with clusters, the member nodes in the cluster usually pass some local security information to the cluster head. Then cluster head makes intrusion decision independently on the basis of the information collected.

Flow 3: In IDS without cluster, there are two ways of detection decision making. One is that the IDS module on one node makes decision directly and issue intrusion alarm. However, this is rarely used in MANET, since local information is often insufficient for making intrusion decisions. Another way is the collaborative decision making.

Appendix 1 illustrated the detailed comparison study on existing methods for intrusion detection for MANET based on inputs, process methods, outputs, advantages and disadvantages. The letters of A through G are related to the letters in Figure 1.

In Appendix 1, the existing intrusion detection methods are presented. Method 1 is efficient and bandwidth-conscious. It targets intrusion at multiple levels and fits the distributed nature of IDS for MANET. The method has clusters and the IDS on cluster head employs independent detection decision-making after gathering information from other nodes. It utilizes mobile agent for the communications among nodes.

Method 2 implements local and collaborative decision making in anomaly detection. In this approach, individual IDS agent works by itself and collaborate in decision making. Each IDS agent runs on a node and monitors local activities. If a node detects locally intrusion with strong evidence, then the node can conclude intrusion happens and then initiate an alarm response. However, if the evidence is not strong enough but needs investigation in a wider area in the network, then the IDS agent can start an collaborate procedure which is a distributed consensus algorithm (Zhang and Lee, 2003).

In Method 3, the authors proposed a cluster-based scheme in which a cluster head is elected by a group of nodes in a neighborhood (citizen nodes) and the head node monitor the citizen nodes. Once the cluster head is elected, then other nodes need to transmit the features it obtains locally to the cluster head. This IDS uses anomaly detection implemented with data mining as its detection technique (Lee, 2002).

In Method 4 each node runs a local IDS. Each node detects intrusion locally and use external data to confirm the detection. The

nodes use mobile agents to communicate and collaborate.

Method 5 implements an IDS which use collaboration mechanism in anomaly detection. In this model, a network is divided into logical zones. Each zone has a gateway node and individual nodes. Individual nodes has IDS agent working and detect intrusion activities individually. Once an individual node detects intrusion, it generates an alert message. Gateway node aggregate and correlate the alerts generated by the nodes in its zone. An algorithm is used in aggregate the alerts based on the similarities in the attributes of the alert. Only gateway nodes can utilize alert to init alarm (Sun, Wu and Pooch, 2003).

Method 6 also utilize cluster and cluster head employs the independent decision making. It also utilizes the mobile agent for communications among nodes. The intrusion detection engine is a case-based agent designed with the principle of artificial intelligence.

Method 7 mainly introduces a detection algorithm which uses the statistics of packets, namely the relations between different features, such as the correlation between the number of packet dropped and the percentage of change in routing table. This algorithm can be used as an intrusion detection engine in other IDS architecture.

In method 8, the normal behavior of critical objects in the Network is constructed into normal specification first. Then the actual behavior is compared to the normal specification. It uses distributed network monitor to trace the request-reply flow in the routing protocol. The network monitor runs a specification based detection algorithm to make decisions (Sekar, 2002; and Okazaki, 2002).

In method 9, the two neighboring nodes of one node are used to ensure that the packets are not modified when traveling in the network. This is done by comparing the information in each packet at each hop. It has two modes: passive mode-to protect a single host and active mode-to collaboratively protect the nodes in a cluster. In active mode, a cluster head starts a voting algorithm to determine whether intrusion really happens.

In method 10, information in the management information base (MIB) is used as input data. It also uses mobile agent and a collaborative decision making mechanism.

3.2 Inputs

Most of the methods take packets and network traffic related information, such as updates in routing table or request-reply flow in the network.

Among the ones that use packets related information, Methods 6 and 9 uses the information inside the packets header directly, such as network address or port number. Other methods using packet or network traffic related information mainly use statistical data processes from packet information, such as the statistics of the number of packets received and sent or the statistics of change in routing table. Method 7 utilizes the statistics derived from packet or traffic related statistics, for instance, the correlation between the number of packets dropped and the percentages of updates in routing table.

Methods 1 and 2, allow the IDS to work on different types of audit data or the possibility to adapt to different types of audit data. This property is valuable and should be an important consideration for the future design of IDS.

3.3 Outputs

Most of the architectures detect only the fact that an intrusion happens. Some methods go further to obtain more information, such as the type of attack and the location of the intruder. For instance, Zone based IDS can detect both the type and location of the attack.

3.4 Cluster Nodes

Some of the methods, such as Methods 1, 3, 6 and 9, utilize cluster head or gateway nodes. The objective of cluster head is that some of the resources consuming computation, such as intrusion detection, can be carried out only on several nodes of

the network. Therefore, most other nodes can focus on real work of network traffic.

The cluster head usually collects information from cluster member to make the detection decision. In some methods, the original input data is further processed or formatted before it is sent to cluster head. By doing this, the network traffic for transferring such data is reduced. The computation on the cluster head can also be reduced because the incoming data from member nodes is already formatted for the IDS use.

The security communication between the cluster head and its member nodes should receive attention of research.

3.5 Local Intrusion Detection

Most of the methods, except Method 8, utilize anomaly detection. The anomaly detection is more suitable than misuse detection in MANET.

In MANET, the anomaly detection has a weakness: the profile of normal behavior need to be updated periodically. This places a heavy burden on the limited network resources. Method 7 can construct anomaly model automatically. This may provide a solution to this weakness.

Method 8 uses specification detection. In theory, the specification detection can detect novel attack type and achieve low false alarm rate.

Method 6 basically utilizes misuse detection.

3.6 Communication Mechanism

All the architectures need some form of communications between IDS running on different nodes. The communication can be done with mobile agents.

Methods 1, 4, 6 and 10 utilize mobile agents. The objective of using mobile agents is to reduce the network traffic and leave more resources for real work of network.

However, in such architecture, when the mobile nodes allow mobile agents to carry out computation on them, they also open a door for attacks. Therefore, the security mechanism that protects nodes from malicious code is very important. And such mechanism may make the mobile agents less powerful and efficient, which is just the one of the important consideration for using mobile agents. Also mobile agent management, such as the creation, migration, operation and termination of mobile agents, is also quite challenging.

Those architectures which do not use mobile agents rely on network protocols to exchange data and collaborate in intrusion decision making. Such protocols need to be secure and robust. At the same time, such communication uses a lots of the bandwidth resources, which is very limited in MANET (Capkun., 2003).

3.7 Collaborative and Independent Decision Making

Methods 2, 5, 9, 10 utilize collaborative decision making in intrusion detection. Others uses independent decision making. Most methods that use clusters, except Method 9 do not use collaborative decision making.

The objective of using collaborative decision making is to include information from different nodes in the decision making so as to make more accurate decision.

The collaborative decision making has some weak points in terms of security. It is more easily under the attacks such as denial of service and spoofed intrusion.

3.8 Advantages and Disadvantages

Method 1 provides a framework to work with multiple types of audit data. It is expandable: if the IDS needs to work with new types of audit data, it can do so by just incorporating extra agents that can monitor the new type of audit data. Unfortunately, its performance is not verified by any implementation. Once its performance is proved to be on an acceptable level, this framework can serve as a generic and expandable architecture for commercial products, since having a possibility to add in more functionality is an important property for successful products. Because it utilizes the cluster heads, it is supposed to make the

MANET more efficient by limiting the resources usage for IDS purposes on only a few nodes. Such framework can be applied in the environments where the security requirement is medium but efficiency requirement is high. Also, it may easily be expanded for multi-layered MANET.

Method 2 provides a framework that fits the distributed nature of MANET. It also works with multiple types of audit data. If the IDS needs to work with new types of data, it can add in more data collection module in the IDS agent. It uses data mining as the local intrusion detection mechanism. The data mining is supposed to be superior both in detection rate and false alarm rate. Also because this IDS does not use mobile agent for communication, it can be designed for high security need, if it can find an effective way to protect from Byzantine nodes. This framework is designed for flat MANET. In a large multi-layered MANET, it can work in a subsection of the MANET.

Method 3 improves the efficiency of MANET by limiting the resources usage for IDS purposes on only a few nodes. The implementation proves it can also achieve satisfactory level of detection rate. Such framework can be applied in the environments where the security requirement is medium but efficiency requirement is high. Also, it may easily be expanded for multi-layered MANET (Debar and Wespi, 2001).

Method 4 provides a scalable architecture by using mobile agents. If the IDS needs more functionality, it can just incorporate more mobile agents with new tasks. It is supposed to reduce network traffic for intrusion detection purpose. However, since this architecture relies heavily on the use of mobile agents, it incurs computational complexity in creating and managing all the agents. This architecture needs an implementation to verify its performance.

Method 5 significantly improve detection rate and reduce false alarm in simulation test. This is the key performance indicator of IDS in MANET. However, there is no data on its run time efficiency: how much resources it needs, especially the CPU time and network bandwidth. Since its algorithm in zone establishment and communication protocols between nodes for intrusion detection purpose seem quite complicated, it is reasonable to believe this architecture should require significant amount of resource. It does not used mobile agent and have gateway nodes which work just like a cluster head. This architecture can be applied in environment where the requirement for IDS performance and security is high and MANET resources are generally available .

Method 6 can automatically construct anomaly model but has high computational costs; Method 7 has low overhead, but was designed only for one routing protocol, and needed modification of protocols; Method 8 is novel with no conventional local detection mechanism, but has low efficiency since packet is checked at each hop; and Method 10 is distributed and efficient in use, with high scalability and can detect attack at multiple levels, but has security and computational cost and management problems related to mobile agents.

4. GUIDELINES

In this section, some guidelines are developed to assist selecting intrusion detection methods in MANET.

Guideline 1: In MANET which requires high detection rate and low false alarm rate and have abundant network resources and computational resources at each nodes, the IDS should use data mining or neural network as the local detection techniques in each node and use collaborative decision making between nodes.

Guideline 2: In MANET where the network resources are limited and security requirement for IDS is not high, mobile agent should be used as the communication mechanism between nodes.

Guideline 3: For IDS whose scalability and security requirements are not high, mobile agent should be used to conduct detection on each node.

Guideline 4: For IDS which can be expanded to work with multiple types of audit data, and security requirement for IDS

is not high, mobile agent should be used to conduct detection on each node.

Guideline 5: Given the nature of MANET, local detection without collecting information from other nodes should not be used. This may introduce high false alarm rate and low detection rate.

Guideline 6: In MANET where the computational resources of nodes is abundant and the attack type and location need to be known, the algorithm to find out attack type and location developed in method 5 can be used.

Guideline 7: In the IDS which utilizes cluster, the original audit data on the member nodes should be processed and formatted for the use of the IDS on cluster head node before the data is sent to the cluster head. This reduces both network traffic and computational need of the cluster head. If the security requirement is not high, mobile agent should be used to work on the member nodes, since it further reduces the network traffic.

Guideline 8: In the MANET which does not have high requirement in false alarm rate, collaborative decision making should not be the preferred mechanism since it is venerable to denial of services and IP spoofing attacks.

5. CONCLUSIONS

The objective of the current research is to provide a big picture of the current state of the research on IDS in MANET, and provide a guideline on how to select intrusion detection methods for IDS in MANET. Specifically, this paper first surveyed the existing literatures about the IDS, the MANET and the IDS for MANET and discussed the requirement of IDS in MANET. Then, a framework comparative study is developed to analyze the IDS architectures proposed in the existing literatures. In the comparative study, the paper discussed the proposed architectures according to their inputs, outputs, process methods, advantages and disadvantages. The process methods analysis is more focused on the architectures of IDS in MANET by whether clustering is used, what communication mechanism among nodes is used, what detection decision making mechanism is used, and what local detection techniques are used. The paper also discussed how the choice of different methodologies affects the properties of the IDS in MANET. Finally, a number of guidelines are proposed on selecting the different intrusion detection methods in MANET. This is the first attempt in such research.

The comparative study of intrusion detection in MANET and the guidelines provide a referential framework in exploring possibility of designing new IDS for MANET for researchers in this area. It can also help the decision makers, such as security officer, who needs to select a proper IDS for their MANET. The results of the current research are useful for educational and industrial professionals who are interested in information systems security in the wireless world.

REFERENCES

Albers, Patrick and Olivier Camp, 2002, "Security in Ad hoc Networks: a general Intrusion detection architecture enhancing trust based approaches." Proceedings of the First International Workshop on Wireless Information Systems.

Brutch, Paul and Calvin Ko, 2003, "Challenges in Intrusion Detection for Wireless Ad-hoc Networks." Proceedings of 2003 Symposium on Applications and the Internet Workshop.

Debar, H. and A. Wespi, 2001, "Aggregation and correlation of intrusion detection alerts." Proceedings of th 4th intl symp on recent advances in intrusion detection, pp. 85-103.

Gartner Group, 2000. "Gartner unveils the shape of the wireless economy", Gartner Press Release, September 11 2000

Gillick, Kevin and Randy Vanderhoof, 2000, "Mobile e-Commerce: market place enablers and inhibitors." Smartcard Forum Annual Meeting.

Guha, R., O.Kachirski and D.G. Schwartz, 2002, "Case-Based Agents for Packet-Level Intrusion detection in Ad Hoc Networks." Seventeenth International Symposium on Computer and Information Sciences.

Huang, Y., W. Fan, W. Lee and P.S. Yu, 2003, "Cross-feature analysis for

detecting ad-hoc routing anomalies." Proceedings of the 23rd International conference on distributed computing systems, pp.478-487.

Huang, Yi-an and Wenke lee, 2003, "A cooperative intrusion detection system for ad hoc networks." Proceedings of the ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN '03).

Kachirski, Oleg and Ratan Guha, 2002, "Effective Intrusion Detection Using Multiple Sensors in Wireless Ad Hoc Networks." Proceedings of the 36th Hawaii International Conference On System Sciences.

Kong, J., H. Lou, K. Xu, D. Gu, M. Gerla, and S Lu, 2002 "Adaptive Security for Multi-layer Ad-hoc Networks." Special Issue of Wireless Communication and Mobile Computing.

Lee, Wenke, 2002, "Applying data mining to intrusion detection: the quest for automation, efficiency, and credibility." ACM SIGKDD Explorations Newsletter. 4, 2, pp.35 - 42.

Marti, S., T. Giuli, K. Lai, and M Baker, 2000 "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks." Proceedings of the Sixth Annual International Conference on Mobile Communication and Networking.

May, Paul, 2001 "Mobile Commerce: Opportunities, Applications, and Technologies of Wireless Business", United Kingdom: Cambridge University Press. p. 6

Mishra, Amitabh and Ketan Nadkarni, 2004, "Intrusion Detection in wireless Ad Hoc Networks." IEEE Wireless Communications, February 2004, pp. 48-60.

Okazaki, Y., I. Sato, and S Goto, 2002, "A new Intrusion detection method based on process profiling." Proceedings of 2002 Symposium on Applications and the Internet.

Puttini, R. S, J-Mr. Percher, L Mé, O Camp, R. of Sousa Jr., C J. Barenco Abbas and L J Garcia Villalba, 2003, "Modular for Distributed IDS in MANET Structures." Proceedings of the 2003 International Conference one Computational Science and Its Applications (ICCSA).

Rajavaram, Sowjanya and Hiren Shah, 2002, "Neighborhood Watch: An Intrusion Detection and Response Protocol for Mobile Ad-hoc Networks." Technical Report, UMBC, October 2002.

Sekar, R, 2002, "Specification-based anomaly detection: a new approach for detecting network intrusions." Proceedings of the 9th ACM conference on Computer and communications security, pp. 265 - 274

Smith, Andrew B., 2001, "An Examination of an Intrusion Detection Architecture for Wireless Ad Hoc Networks." Proceedings of the 5th National Colloquium for Information System Security Education.

Stefan Axelsson 2000, "Intrusion Detection Systems: A survey and Taxonomy. " Retrieved on March 26 1004 at Citeceer.com.

Sun, B, K. Wu, and U. Pooch, 2003, "Routing anomaly detection in mobile ad hoc networks." Proceedings of the 12 th International conference on computer communications and networks, pp 20-23.

Sun, bo, Kui Wu, and Udo Pooch, 2003, "Alert aggregation in mobile ad hoc networks." Proceedings of the 2003 ACM workshop on Wireless security, pp.69 – 78.

Tseng, Chin-Yang and Poomima Balasubramanyam, 2003, "A specification-based intrusion detection system for AODV." ACM Workshop on security of Ad Hoc and Sensor Networks

Wei, J., L. Liu, and K. Koong, 2003, "A Framework for Delivering Mobile Commerce Security System." Proceedings of International Conference for Pacific RIM Management: ACME Transaction.

Zhang, Yongguan and Wenke Lee, 2000, "Intrusion detection in wireless ad-hoc networks." Proceedings of the 6th annual international conference on Mobile computing and networking , pp.275 – 283.

Zhang, Yongguan and Wenke Lee, 2003, "Intrusion detection techniques for mobile Manet." ACM/Kluwer Wireless Networks Journal (ACM WINET), 9, 5, pp.545 – 556.

Zhou, L. and Z.J. Haas, 1999, "Securing ad hoc networks." IEEE Network, 13(6), pp 24-30.

Appendix 1. Comparison Study on Intrusion Detection Methods

Number	Method	Reference	A: Input	B: Output	Methodology								Advantages	Disadvantages
					C: Grouping Nodes		D: Communication Mechanism		E: Independent	F: Collaborative	G: Local detection			
					cluster head	zone head	mobile agent	network message			anomaly	misuse	specification	
1	Mobile Agent based IDS	(Kachirski and Guha, 2002).	network packet, system or program level audit data	intrusion alarm and response	yes		yes		yes		yes			Mobile agent's security is hard to implement.
2	Local and collaborative decision making IDS	(Zhang and Lee, 2003)	audit data collected on local nodes, such as updates in routing table	intrusion alarm and response				yes		yes	yes			Vulnerable to Byzantine nodes. Decision making is majority vote. Not implemented and verified.

Appendix 1. Comparison Study on Intrusion Detection Methods (Continued)

Number	Method	Reference	Methodology									Advantages	Disadvantages
			A: Input	B: Output	C: Grouping Nodes		D. Communication Mechanism	Decision Making		G: Local detection			
								E: Independent	F: Collaborative				
3	Cluster head in a cooperative IDS framework	(Huang and Lee, 2003)	Statistics on the number of packets received and sent and on the number of route control messag e.	intrusion detection alarm	yes		yes	yes		yes		Improve the efficiency of IDS in terms of CPU usage and network overhead, Identify attack type.	Need to prevent a compromised node be elected as cluster head; Not mention false alarm rate
4	Local Intrusion Detection System	(Albers and Camp, 2003).	Audit data in Management Information DB (MIB)	Intrusion alarms.			yes	yes				Less network traffic, scalable	Complexity in mobile agents creation and management
5	Zone based IDS (ZBIDS)	(Sun, Wu and Pooch, 2003)	Statistics of data in routing table.	Intrusion alarm with Identified intrusion type and location.	yes		yes		yes	yes		Reduce false alarm and improve detection, incorporate multiple intrusion techniques.	Complicated architecture needs many protocols to coordinate; computation to establish zones is complicated.

Appendix 1. Comparison Study on Intrusion Detection Methods (Continued)

Number	Method	Reference	Methodology								Advantages	Disadvantages
			A: Input	B: Output	C: Grouping Nodes		E: Communication Mechanism	Decision Making		G: Local detection		
								E: Independent	F: Collaborative			
6	Case-Based Agents for Packet-Level Intrusion detection	(Guha and Schwartz, 2002)	packet information: network addr, ports and etc	intrusion alarm	yes		yes			yes	efficient, bandwidth-conscious, take into account of the distributed nature of MANET	Mobile agent's security is hard to implement, packet drop rate increase when network load increase, need to improve
7	Cross-Feature Analysis	(Huang, Lee and Yu, 2003)	packet statistics, such as the relations between the packet droped and the change in routing tables	intrusion alarm					yes		automatically construct anomaly model	high computational cost
8	Specification based	(Tseng and Balasubramanyam, 2003).		request-reply flow in routing protocol			yes			yes	low overhead	designed only for one routing protocol, need modify protocol to let the ID work

Appendix 1. Comparison Study on Intrusion Detection Methods (Continued)

Number	Method	Reference	A: Input	Methodology							Advantages	Disadvantages
				B: Output	C: Grouping Nodes		D: Communication Mechanism	Decision Making		G: Local detection		
								E: Independent	F: Collaborative			
9	Neighborhood Watch	(Rajavaram and Shah, 2002)		intrusion alarm at single nodes level; at mutli nodes level, a voting is used to determine alarm		yes	yes		yes		novel, no conventional local detection mechanism	low efficiency since packet is checked at each hop
10	Modular Architecture	(Puttini and Percher, 2003)	(management information base(MIB)	intrusion alarm			yes		yes		distributed, efficient in network using because on raw data is passed, only high level messages passed; scalability; can detect attack at multiple level: system, network and application level	problems pertaining Mobile agents: security, computational cost and management