Ranger, a Novel Intrusion Detection System Architecture for Mobile Ad Hoc Networks

Yinghua Guo
Institute for Telecommunications Research
University of South Australia
Adelaide, Australia
Yinghua.Guo@postgrads.unisa.edu.au

Steven Gordon
Institute for Telecommunications Research
University of South Australia
Adelaide, Australia
Steven.Gordon@unisa.edu.au

***Abstract*— The proliferation of wireless communication and mobile computing is driving the emergence of Mobile Ad hoc Networks (MANETs) with wide application ranges from civilian environment to military communication. However, securing MANETs is a highly challenging issue due to their inherent characteristics. Intrusion detection is an important security mechanism, but little effort has been directed towards efficient and effective architectures for Intrusion Detection System (IDS) in the context of MANETs. We investigate existing IDS architecture design issues, and propose a novel mobile agent based IDS architecture that has each node implementing basic IDS functions, while ranger agents roam the network executing more advanced IDS functions. This is suited to MANETs because it avoids the single point of failure problem, minimises communication overheads at the same time as providing up to date information for intrusion decisions.**

I. INTRODUCTION

A. Motivation

Mobile ad hoc networks are complex distributed systems that comprise wireless mobile nodes that can freely and dynamically self-organise into arbitrary and temporary, ''ad-hoc'' network topologies. They allow people and devices to seamlessly internetwork with no pre-existing communication infrastructure and central administration [1]. Securing MANETs is a highly challenging issue, much more difficult than securing traditional infrastructure-based (wired or wireless) networks. The challenges come from MANET's unique characteristics: unreliability of wireless links, dynamic topology, and absence of underlying infrastructure.

A common approach to securing networks is to use preventive mechanisms: encryption of data traffic; public and private keys for identification and authentication [2]; etc. This can be seen as a first wall of defense against network intruders. The second wall of defense is intrusion detection. Intrusion detection can be defined as the automated detection and subsequent generation of alarms to alert the security administrator in any situation where intrusions have taken, are taking, or about to be take place. It is generally accepted that preventive mechanisms on their own are not sufficient for a network with even a moderate level of security requirements. Continuing advances by intruders, holes in current preventive mechanisms and possibility of attacks from within the network mean the ability to detect (and adequately respond to) an intrusion is vital. Since Anderson's and Denning's milestone work [3, 4], intrusion detection (ID) has received extensive research effort, and a large number of research prototypes have been proposed whose surveys can be found in [5, 6]. However, the characteristics of MANETs make most of these existing IDSs redundant, and motivate effort for producing new architectures for intrusion detection in MANETs.

B. Intrusion Detection in MANETs

In order to identify either an outside intruder who has broken into the protected network, or an inside intrusion, IDSs perform the following tasks: monitoring the network; analysing collected audit information; identifying intruders; issuing alarms; tracking down attackers to prevent such attacks in future, and initiating responses. This functionality is encapsulated in several components (Fig.1): Audit Data Collection (ADC), Audit Storage/Pre-process (ASP), Detection Engine (DE), Response (RES), all of which are controlled by the System Configuration component.

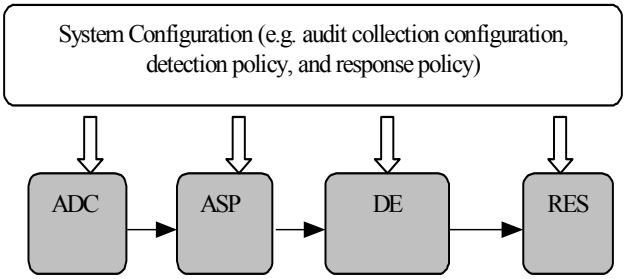

Figure 1. IDS functionality components illustration

Existing IDS prototypes can be classified according to different criteria. One commonly used classification is based on detection methodology: anomaly detection IDS or misuse detection IDS [5]. In this paper, we however concentrate on the architecture issues, assuming either of the detection methodologies can be applied.

1) Host vs Network Based Intrusion Detection

Host-based intrusion detection is the first area explored in the intrusion detection community. Each host runs an IDS independently and there is no cooperation between the systems. In computer networks, such standalone systems where only

intrusions local to a computer can be detected, host-based IDSs are insufficient. Hence Network-based Intrusion Detection Systems (NIDSs) [7, 8, 9] were developed. NIDSs are distributed in nature, i.e. IDS's components, or individual IDSs are placed at different points in the network, and cooperate with each other to make an intrusion decision. The networking architecture could be implemented in various ways. One possible way is that audit collection components are distributed in the network, and intrusion decision is made at a central node. Alternatively, both audit collection and intrusion decision components are distributed in the network.

2) Distributed vs Centralised Intrusion Detection

The networking architecture can be classified based on where the intrusion decision is made. An IDS architecture can be Distributed and Dictatorial (DAD) or Distributed and Cooperative (DAC). While they both distribute audit data collection components through the network, the intrusion decision is made dictatorially by a centralised host in the DAD architecture, and made cooperatively by participating hosts in the DAC architecture.

3) Flat vs Hierarchical Intrusion Detection

The networking architecture can also be classified based on the distribution of functionality amongst nodes, e.g. flat or hierarchical. In the flat architecture, every node in the network on which IDS runs is considered equal and plays the same roles equally: audit collection and/or intrusion decision. On the other hand, nodes in the hierarchical IDS architecture are differentiated as control component at the root, information aggregation components, and operational components at the leaf, performing ID functionalities: intrusion decision, audit data pre-processing, and audit data collection, respectively.

C. Our Proposed Architecture

Though many IDS architectures have been designed for infrastructure-based networks, they are not applicable in MANET environment. Motivated by this consideration, we propose a novel mobile agent based IDS architecture particularly suitable to MANETs. The main contribution of our approach is the mobile IDS agent detector, namely *ranger*, patrolling in the network. By utilizing rangers, our proposed architecture is effective, efficient and attack tolerant. Another advantage of our approach is the seamless security adaptation corresponding to various application scenarios. This benefit comes from flexible modular design of ranger.

D. Overview of the Paper

This paper is organised as follows: Section II reviews the existing IDS architectures in MANETs, and presents their evaluation. In section III, we provide a detailed description of our proposed IDS architecture. Comparison and discussion between our proposed IDS architecture and other current approaches are given in section IV. Finally, we conclude in section V and present our future work.

II. Previous Work

There has been significant research effort directed towards intrusion detection in wired networks over recent years. This includes architecture models for IDS. However the characteristics of MANETs limit the applicability of these IDS architectures. In this section we review and evaluate IDS architectures proposed in MANET.

A. Proposed IDS Architecture Models in MANETs

In their pioneering work, Zhang and Lee described a distributed and cooperative intrusion detection model for MANETs [10]. In their model, IDS is configured in a flat architecture, in which each IDS agent residing at each mobile node is considered as equal and performs the same intrusion detection functionalities independently. Intrusion detection is executed in the DAC manner. Each IDS agent looks for suspicious activities on the node. If an anomaly is detected with strong evidence, this agent will then initiate an appropriate response. However, if an anomaly is detected with inconclusive evidence, neighbouring IDS agents cooperatively participate in the decision of such anomaly via a majority voting algorithm.

Smith suggested a mobile agent-based IDS architecture for wireless ad hoc networks in [11]. Similar to [10], the proposed IDS was also designed in flat manner. Intrusions can be detected either based solely on the data in the local intrusion database by an individual mobile IDS agent, or by cooperating with other mobile IDS agents. The difference between this model and [10] lies in the cooperation paradigm: the IDS agents in [10] are static and obey the RPC paradigm, on the other hand, [11] utilises mobile agents (MA) to implement the cooperative detection and response. The benefit from utilising MA includes: overcoming network latency, communication overhead reduction, scalability, etc [14].

Reference [12] presents a general intrusion detection architecture for MANETs, and its basic principle is DAC mechanism, same as one described in [11]. One novelty of this work is its use of SNMP data in MIBs as audit sources.

Another mobile agent based IDS architecture is proposed for wireless ad hoc networks in [13]. Differing from those architectures given in [11, 12], mobile IDS agents in this architecture are no longer considered equal, and instead they are designated specific IDS tasks according to their functionality, and as a whole, the IDS architecture is modular and hierarchical. Specifically, while some IDS agents (residing on leaf nodes) are responsible for monitoring system-level and application-level activities, other IDS agents (residing on root nodes) have the capacity of network packet monitoring and network-level intrusion decision. In this architecture, intrusion detection is carried out in a slight variation from the DAC mechanism, where if inconclusive anomalous activity is detected on a node, the node is reported to the decision agent on the root node for further decision instead of convening neighbouring nodes to participate in this decision.

B. Discussion and Evaluation of Current IDS Architectures

All of the above IDS architectures generally fall in two categories: flat [10-12] and hierarchical [13] architecture. This section presents an evaluation of these proposed architectures.

1) Effectiveness

Naturally, an IDS architecture is expected to be effective in that it can carry out the intrusion detection task accurately,

completely and timely. The high IDS effectiveness is primarily based on the applied Intrusion Detection (ID) algorithms, algorithm execution method, and algorithm's input (e.g. network traffic, host audit data). In the proposed IDS architectures, ID algorithms could be executed either in a centralized way [13] in which the suspicious activities are detected by a certain node, or in the DAC way [11] where identifying intrusions is accomplished cooperatively by multiple participating IDS agents. Whether the DAC algorithm execution is performed properly and effectively relies on both individual ID execution success of each participating IDS agent, and correct coordination and interaction (such as information sharing, individual execution combination) among them. Any flaw or functional incorrectness of such participating components will degrade effectiveness performance of the whole DAC intrusion detection execution. From this aspect, the hierarchical architecture has advantage over the flat architecture because the former implements intrusion decision (ID algorithm execution) centrally, which avoids complicated coordination and interaction. This also allows hierarchical architectures to identify and initiate responds to intrusions faster.

2) Efficiency

Beside effectiveness, efficiency is another metric for evaluating the design of an IDS architecture. When an IDS is being used, both network resources (e.g. bandwidth) and host resources (e.g. CPU capacity, memory, battery power) are being consumed. An efficient IDS architecture should minimise the consumption of these resources. Compared with the hierarchical architecture [13], the flat architecture [11] is relatively inefficient, especially in large-scale and/or resource limited networks due to the following two reasons:

- Considerable bandwidth consumption raised by exchanging data and code among multiple IDS agents for detecting intrusions and triggering response;
- Overuse of host resources by performing duplicated IDS functions at every node rather than allocating specific ID functions to different nodes.

3) Self-Security

Since present IDS architectures designed for MANETs are distributed in nature, they are not secure if any of their components are insecure. This may be so if there is a Single Point of Failure (SPF) or the IDS input is tainted.

In a hierarchical architecture, the IDS functions are often located on one or a few selected nodes. Accidental or malicious shutdown of these nodes may cause the entire IDS to fail.

The input data used by ID algorithms is vital for an effective and secure IDS. If this input data is insecure (e.g. open for modification by attackers), then the IDS can be rendered useless. Although both hierarchical and flat architectures are susceptible to corrupted input data, the former suffers more from it. This is because in the hierarchical architecture, all key intrusion relevant information are sent to the root nodes for further analysis, and therefore there is an increased likelihood of capture and subsequent modification of such information by knowing the location of the root nodes in the hierarchy (e.g. through eavesdropping and analysing information flow). In the flat architecture, however, it is more difficult to capture the key information since it is distributed among participating IDS nodes, and even if one IDS node is compromised, the attacker can only get part of the key information.

III. RANGER, A NOVEL IDS ARCHITECTURE FOR MANETS

Given various trade-offs between the architectural options for IDS in MANETs, and taking into account the capabilities and limitations of existing models, we propose the Ranger IDS architecture for MANETs. Ranger is built on a mobile agent framework, differing from the conventional flat or hierarchical IDS architecture in that intrusion detection is executed by a certain number of mobile IDS agents, called rangers. By using rangers, our proposed architecture solves two common problems existing in a hierarchical architecture – scalability and (some aspects of) self-security – while at the same time avoids degradation of efficiency and effectiveness often caused by complex cooperative ID mechanisms in a flat architecture.

Our architecture consists of two major components:

- A ranger that roams the network performing intrusion decisions at nodes and updating IDS information;
- A stationary light-weight IDS agent, called garrison, that resides on each node.

A. Garrison, Stationary IDS Agent

Each node in the network hosts a stationary IDS agent. This agent is designed to be lightweight, which means it only has limited and basic missions to carry out and consumes as few resources as possible. This is particularly important in the MANET context, where host resources may be severely constrained. Each garrison has five function modules (Fig.2): Local Monitoring and Auditing, Stationary Information Database, Primary Intrusion Detection, Mobile Agent Communication, and Local Intrusion Response.

1) Local Monitoring and Auditing(LMA)

This module is responsible for monitoring network traffic in/out of the host and collecting audit data. The choice of audit data may be affected by: the type of intrusions we wish to detect; detection mechanism used; and systems in which the detection will be done. After being pre-processed (e.g. filtering, format transforming), the data is passed to the PID module for primary intrusion decision. In addition, when a ranger docks to a stationary agent, a copy of the local audit data is sent to the ranger through the MAC module for mining profiles of normal activity (see Section III. B).

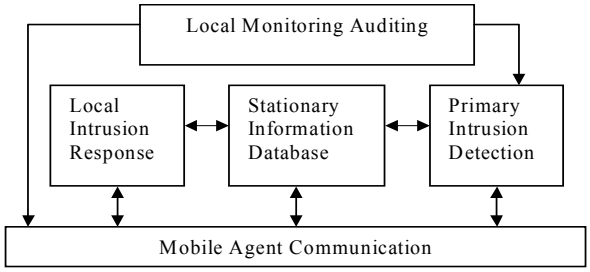

Figure 2. Function modules of a garrison

2) Stationary Information Database(SID)

The stationary information database maintains information necessary for intrusion decision and response. This information can be categorised into two classes:

- For intrusion decision, such as known attack signatures and profiles of normal user activity.
- For intrusion response, e.g. response policy.

The SID on each node is updated with the latest information by rangers when they attach to the garrison. With reference to this database, the PID module analyses input audit data from the LMA and identifies intrusions.

3) Primary Intrusion Detection(PID)

This module is a place where audit data is processed and intrusions are identified. In order to deal with a large spectrum of attacks effectively and flexibly, this module must allow multiple detection algorithm implementations to be used and/or selected based on the type of attacks being addressed and the application environment.

If an anomaly is detected by the PID module with strong evidence based on the data in the SID module, the LIR module initiates an appropriate response to the identified intrusion. If the data in the SID is not sufficient to determine if the present activity should be classified as an intrusion, then the PID will call for rangers to come for further analysis through the mobile agent communication module.

4) Mobile Agent Communication(MAC)

The MAC module is necessary to enable stationary IDS agents to communicate with rangers. As a flexible module, it is also installed in rangers for communication. Through this communication media, garrisons can call for rangers, and rangers can come to interact with garrisons for further intrusion identification or information updates. One basic approach for communication is for garrisons to broadcast (flood) the network in search for a ranger when it is needed. However, more efficient techniques, such as service discovery protocols and/or regular location updates, should be considered for larger networks. To maintain the security of the IDS, this module should use secure transmissions.

5) Local Intrusion Response(LIR)

With the guidance of response policy stored in SID, the local intrusion response module is responsible for initiating response actions when an intrusion is confirmed. Current possible automated response mechanisms range from (passive) notification and (active) attacker filtering. Examples of such response actions include shutting down the node in question, or disconnecting the node and attackers, or excluding compromised nodes by re-initialising communication channels between them and other nodes.

B. Ranger, Mobile IDS Agent

In our proposed architecture, rangers are mobile IDS agents that roam in the network and perform key IDS functions as in a hierarchical architecture. A ranger consists of four main function modules (Fig.3): Mobile Information Database, Intrusion Detection Confirmation, Normal Profiles Computation and MAC. Critical IDS missions executed on rangers include: (1) computing user profiles using trace data collected from garrisons, and obtaining latest attack patterns and response policies from system administrators (2) updating garrisons with latest intrusion information, (3) answering requests raised by garrisons, and (4) analyzing intrusions further on the scene.

1) Mobile Information Database(MID)

A ranger visits a garrison in two ways: visiting a garrison upon receiving its calls for ID confirmation, or visiting a garrison randomly during patrolling in the network. In both cases, when a ranger docks to a garrison, it utilizes audit data collected by garrison to calculate new profiles of normal uesrs. Moreover, rangers may obtain latest attack patterns and response policies from system administrators. Therefore, in the process of roaming in the network, rangers could gather global intrusion information by visiting multiple hosts. Compared with the same kind of information stored in SID module in each garrison, information maintained in MID is more comprehensive and latest, and therefore helpful to confirm suspicious intrusions.

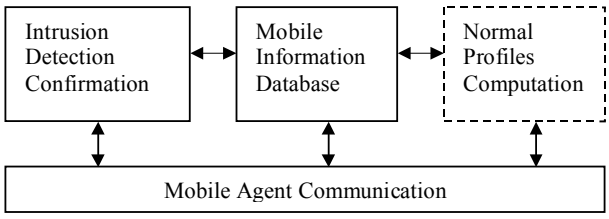

Figure 3. Function modules of a ranger

2) Intrusion Detection Confirmation(IDC)

This module functions similarly to the PID module in garrisons. The difference is that the IDC module makes intrusion decision on the base of information stored in MID module, which is more comprehensive and up to date than that in garrison's SID. Additionally, to deal with multifarious attacks, the IDC module is designed in a modular manner: it can be installed/uninstalled with various detection algorithm models corresponding to various attacks in different environments. In short, being a lightweight agent, garrisons are only charged with primary IDS missions (i.e. executing basic detection algorithms). Rangers, equipped with more comprehensive information and detection algorithms, patrol the network and settle in a garrison for intrusion confirmation when it is necessary.

3) Normal Profiles Computation(NPC)

The normal profiles computation module is a place to mine profiles of normal user activities for anomaly detection. When a ranger resides on a garrison, this module, using trace data collected from the garrison, computes profiles with certain computing algorithms [4, 10]. Designed as a pluggable module, the NPC could be installed to rangers in certain application scenarios, and be plugged out in other scenarios (see section IV.A for more details)

C. Intrusion Detection Process

In our proposed IDS architecture as shown in Fig.4, each mobile node hosts a stationary IDS agent (garrison) performing local monitoring, auditing, and primary detection. In addition,

when the network is being initiated, a pre-defined number of rangers equipped with appropriate function modules are dispatched with certain mobility adapting to application environments. By comparing audit data with intrusion information stored in the SID module, the garrison looks for suspicious activities on the node it resides. If an anomaly is detected with strong confidence, the LIR module initiates appropriate response to it. If, on the other hand, the data in the SID is not sufficient to identify intrusions, then the PID will call for rangers to come for further analysis through the MAC module. Patrolling the network, rangers will visit those garrisons who have not sufficient evidence to identify intrusions. When rangers dock to a garrison, they will make final intrusion decision based on the latest information stored in their MID modules. At the same time, these rangers will interact with each other to make their intrusion information consistent. In addition, when a ranger moves to a garrison during normal operation (i.e. not in response to a request), the ranger uses trace data collected from the garrison to compute profiles, and obtains latest attack patterns and response policies.

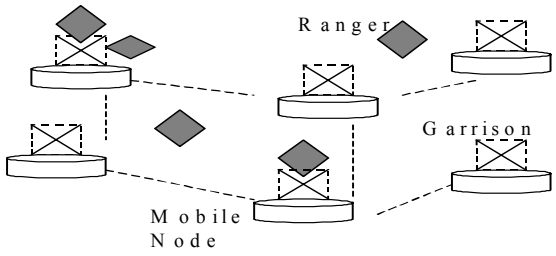

Figure 4. IDS architecture for mobile ad hoc networks

IV. DISCUSSION

A. Properties of Ranger

Our proposed IDS architecture has several key properties distinguishing it from other IDS architectures:

1) Seamless Security Level Adjustment

In general, various application environments have different security requirements for their underlying communication networks. MANETs, for example, are required to be protected with higher security level when they are deployed in hostile and harsh environment (i.e. military applications) where network's availability and security are the first things to consider. On the other hand, the requirement of communication security in civilian applications is comparatively low. In some cases, it is desirable that security level of MANETs provided by IDSs should be adjusted elastically and seamlessly corresponding to application scenario transformation. For instance, one military group is carrying out a rescue operation in the rear area of battlefield that is a comparatively non-hostile environment. In this case, MANET is protected by IDS only with ordinary security level. At this moment, if this group is dispatched to the battlefront for an emergency mission, the IDS should be configured to provide higher security level accordingly, and this adjustment of security level is desired to be autonomous and seamless. So far, to the best of our knowledge, all the proposed MANET IDS architectures are designed to protect MANETs in a certain application environment, and none of them can provide flexible and adaptive level of security provisioning.

Our proposed IDS architecture is designed to be a seamlessly adaptive approach that is able to adjust security provision level according to different application scenarios automatically without any outside interference. The adaptation property is represented by pluggable units (i.e. NPC module, detection algorithm models), the adjustable number of rangers, and their mobility. When MANETs are deployed in security sensitive environment, our IDS is configured in a "heavy loaded" manner to provide high level security provisioning: increase the number of roaming rangers, increase their mobility, and install more specific pluggable units. On the other hand, our IDS architecture could be "light loaded" (i.e. less roaming rangers, little mobility and less pluggable units) to protect MANETs in low security environments. Finally, the change of different security provisioning levels is achieved seamlessly. At the network initialisation stage, rangers are dispatched with sufficient intelligence and autonomy to change the security level when needed, such as install or uninstall pluggable units, eliminate/retrieve rangers, and increase/decrease their mobility, without any outside interference.

2) Attack tolerance

In addition to protecting communication networks, IDS should defend itself against attacks. However, current IDSs in MANETs do not address this issue effectively: hierarchical IDS architectures possess the SPF security flaw, and flat IDS architectures address this problem at the cost of complex cooperative mechanisms leading to depletion of resources. Our proposed architecture solves this problem from a new aspect: rangers keep roaming in the network, and their non-predictive mobility will cloak them from attackers' sniffing or orientation. Therefore, it is reasonable to believe that rangers could avoid attacks since it is difficult for attackers to capture (or find) them. Furthermore, rangers are designed in a flexible and modular manner so that each individual ranger might use different ID algorithms when it was dispatched. This is helpful to avoid the following situation: in a uniform IDS agent configuration environment where all IDS agents perform the same ID algorithms, an adversary who is able to find a way to avoid detection at one agent, will exist in the network without being detected by other agents. Hence, in our architecture, even if one ranger is compromised, other surviving rangers will inform each other to isolate the compromised ranger and exclude it. More importantly, the remaining rangers will likely detect the intruder and gather knowledge of the detection schemes which have been compromised.

B. Comparison with Other Approaches

Here we compare our approach with current IDS architectures for MANETs in terms of effectiveness, efficiency, and security. We consider these metrics for each of the three major IDS's components: intrusion information acquisition, intrusion detection, and intrusion response.

1) Intrusion information acquisition

Intrusion information is the basis of IDS functions. Its acquisition consists of collection, exchange and update. The way in which information is acquired can have significant impact on IDS architecture performance. While each IDS agent in [12] accomplishes intrusion information exchange and update in the DAC manner where each of them broadcasts its local information to other participating agents, in our proposal the information update is made by rangers visiting garrisons. It is clear that, in large-size networks, the DAC mechanism is less efficient than Ranger due to the reason that repetitious and frequent broadcasting by all the participating hosts throughout the network is very resource consuming, but a limited number of rangers moving between nodes consume comparably less resources. On the other hand, in small-size networks, our approach also has efficiency advantage over the DAC approach: while DAC mechanism only provides a fixed level of security at a given resources consumption level, Ranger can adjust the information acquisition approach (heavy loaded or light loaded) to adapt to the different security requirements in various application scenarios. Compared with [13], Ranger should be more effective since each IDS agent in [13] only has local information, whereas in our architecture garrisons can gather more information over time when rangers dock to them. Additionally, as Ranger does not have the SPF problem existing in [13], it is more tolerant of attacks against itself.

2) Intrusion detection

Differing from the DAC intrusion detection mechanism applied in [12] and [11], if a stationary IDS agent has inconclusive evidence in our approach it will request rangers to come to the node to make a final intrusion decision. In other schemes, the DAC approach involves significant information exchange to maintain a coordinated view for a final intrusion decision. As network size grows, this coordination will become excessive, and as a result degrades the effectiveness and efficiency performance of [12] and [11], especially in resource limited networks. In our architecture, the final decision is requested by a garrison when it is needed, and is made by rangers on the node in question so as to avoid the complicated interaction and coordination among nodes. Moreover, to complete interaction and coordination, necessary information needs to be exchanged among participating nodes. The more information exchanged, the longer the procedure of information transmission, and subsequently there is a higher possibility that such information is exposed to attackers and could be eavesdropped, interrupted, and subverted. Therefore for the security of the IDS itself, Ranger is more attack-tolerant than [12] and [11]. Finally, our approach has security advantage over the hierarchical architecture [13] because of the absence of SPF problem.

3) Intrusion response

Reacting to intrusions in a timely manner is a key feature of any IDS architecture. In [12] and [11] a global response needs a relative long procedure because it is initiated in the DAC manner involving time-consuming interaction and coordination among participating IDS agents. Our architecture can react to intrusions more timely because response is launched by rangers on the scene – the only significant delay is locating the ranger, and the ranger moving to the garrison. Similar to its intrusion decision procedure, [13] appoints global response initiation function to the root node(s). This makes response actions in [13] less reliable than our architecture because of the potential vulnerability of the single point (root node)

V. CONCLUSION AND FUTURE WORK

This paper investigates the existing architectures for intrusion detection systems in MANETs and proposes a new architecture that allows seamless adaptation between security levels and tolerance to attacks by not relying in central nodes. The architecture locates basic intrusion detection functionality on all nodes, and uses mobile agents for additional functionality to move around the network when needed. It also provides a flexible balance between effectiveness, efficiency and tolerance to attacks.

Future work will include research into the seamless adaptation property, e.g. a mechanism to recognize the application environment and selecting suitable parameters (e.g. number of rangers, degree of mobility). In addition, the reaction of rangers when one of them is compromised needs to be studied, such as how to know one ranger is compromised. Finally, after developing each mechanism in further detail, performance analysis of the architecture needs to be conducted.

REFERENCES

[1] I.Chlamtac, M. Conti, Jennifer J.-N. Liu., Mobile ad hoc networking: imperatives and challenges, Ad Hoc Networks, 1 (2003), 13-64.

[2] B.Schnerer, Secrets and Lies: Digital Security in a Networked World, John Wiley & Sons, Inc, New York, 2000.

[3] J. P. Anderson, Computer Security Threat Monitoring and Surveillance, Technical Report, Co., Fort Washington, April, 1980.

[4] D. E. Denning, An Intrusion-Detection Model. IEEE Transactions on Software Engineering, Vol. SE-13 (No.2):222-232, Feb. 1987.

[5] S. Axelsson, Intrusion Detection Systems: A Taxomomy and Survey, Tech. report No. 99-15, Dept. of Comp. Eng., Chalmers Univ. of Technology, Sweden, 2003.

[6] E. Lundin, E. Jonsson, Survey of Intrusion Detection Research, Tech. report No. 02-04 Dept. Comp. Eng., Chalmers Univ. of Technology, Sweden. 2004.

[7] T. Heberlein, et al. A Network Security Monitor, In Proc. IEEE Symp. Research in Security and Privacy, pp. 296-304, 1990.

[8] B. Mukherjee, L T. Heberlein, and K. N. Levitt, Network Intrusion Detection. IEEE Network, 8(3): 26–41, May/June 1994.

[9] S. R. Snapp, et al, The DIDS (Distributed Intrusion Detection System) prototype. In Proc. Summer USENIX Conference, pp. 227-233, San Antonio, Texas, 8-12 June 1992.

[10] Y. Zhang and W. Lee, Intrusion Detection in Wireless Ad Hoc Networks, in Proc. MobiCom, pp. 275–28, Aug. 2000.

[11] A. B. Smith, An Examination of an Intrusion Detection Architecture for Wireless Ad Hoc Networks, 5th Nat'l. Colloq. for Info. Sys. Sec. Education, May 2001.

[12] P. Albers et al., Security in Ad Hoc Networks: a General Intrusion Detection Architecture Enhancing Trust Based Approaches, 1st Int'l. Wksp.Wireless Info. Sys., Ciudad Real, Spain, Apr. 3–6, 2002.

[13] O. Kachirski and R. Guha, Intrusion Detection Using Mobile Agents in Wireless Ad Hoc Networks, Knowledge, In Proc. IEEE Wksp. Media Net, pp. 153–58, July 10–12, 2002.

[14] W. Jansen et al., Applying Mobile Agents to Intrusion Detection and Response, National Institute of Standards and Technology Computer Security Division, NIST Interim Report (IR) – 6416, October, 1999