A Cluster-Based Distributed Hierarchical IDS for MANETs

B. Pahlevanzadeh, S.A. Hosseini Seno, T.C. Wan, R. Budiarto, Mohammed M. Kadhum
NAv6 Center, School of Computer Sciences, Universiti Sains Malaysia (USM), Penang 11800, Malaysia
Graduate Department of Computer Science, College of Arts and Sciences, Universiti Utara Malaysia, 06010 UUM Sintok
Emails: {bahareh, hosseini, tcwan,rahmat@nav6.org; kadhum@uum.edu.my}

Abstract-**Many attempts were made to secure *wireless ad hoc networks*, but due to special ad-hoc nature, which is lack of a fixed infrastructure and central management, finding an optimal and comprehensive security solution is still a research challenge. Intrusion detection system is one of key techniques and best solution instead of intrusion protection behind protecting a network against intruders on mobile ad hoc network. In this paper, we introduce background knowledge of *mobile ad hoc networks* as well as *intrusion detection systems* and *mobile agents*. After investigating of existing intrusion detection based on mobile agents for wireless mobile ad hoc network; based on our best knowledge from previous researches, we design cluster-based distributed hierarchical intrusion detection system using mobile agents over *Cluster-Based Routing Protocol (CBRP)*. The unique features of CBRP are the main factors of our success in achieving our goal to propose some enhancement based on the characteristics and measure the efficiency of intrusion detection system in term of bandwidth utilization and energy consumption.**

I. INTRODUCTION

With improvement of wireless ad hoc network applications and mobile devices, security becomes one of the main problems, which ad hoc networks face nowadays. Just like any other network, ad hoc networks experience common security vulnerabilities that cause attacks such as denial of service attack, intruding, spoofing, eavesdropping and signal jamming. Furthermore, preservation of security, reliability, intentional jamming and latency are considerable in a wireless ad hoc network [1].

Mobile ad hoc network (MANET) has unique characteristics that make it more vulnerable to several types of attacks and physical security threats than fixed wired networks. Some of these characteristics include mobility, energy conservation, decentralized network topology, bandwidth and physical security limited. Besides of these characteristics, understanding potential type of attacks is usually the first step towards developing good security solutions. Generally, attacks in ad hoc network can be divided into two classes, passive attacks and active attacks. The passive attacks in routing protocol is eavesdropping only, but not endangering message transmission. The active attacks can be classified into two classes, external attacks and internal attacks. Internal attacks are more severe attacks because internal nodes have all necessary certificates for authentication and so on. These characteristics impose heavy limitation on functionality of an effective intrusion detection system (IDS) as a second line of defense [2]; therefore securing wireless ad hoc networks are a highly challenging issue.

The main scope of our work is new design and implements of efficient distribution of mobile agents with specific IDS tasks according to their functionality over a MANET over CBRP. This model expected to cover the effective IDS requirements especially accuracy to explore the development of security in a MANET [3].

II. BACKGROUND

A. Cluster Based Routing Protocol

CBRP is a routing protocol designed to be used in mobile ad hoc networks. The protocol divides the nodes of the ad hoc network into a number of overlapping or disjoint 2-hop diameter clusters in a distributed manner. Each cluster chooses a head to retain cluster membership information. Based on cluster membership information kept at each cluster head, inter-cluster routes are dynamically discovered. The protocol efficiently minimizes the flooding traffic during route discovery and speeds up this process by clustering nodes into groups. Moreover, the existence of uni-directional links and the use of these links for both intra-cluster and inter-cluster routing are extremely considered by the protocol. An example of an ad hoc network is shown in Fig. 1. Nodes are organized to five clusters and each of them has a cluster head.

Unlike the other on-demand routing protocols, in CBRP the nodes are organized in a hierarchy. Cluster-head coordinates the data transmission within the cluster to other clusters. The advantage of CBRP is that only cluster heads exchange routing information, therefore the number of control overhead transmitted through the network is less than the traditional flooding methods. However, as in any other hierarchical routing protocol, there are overheads associated with cluster formation and maintenance [4].

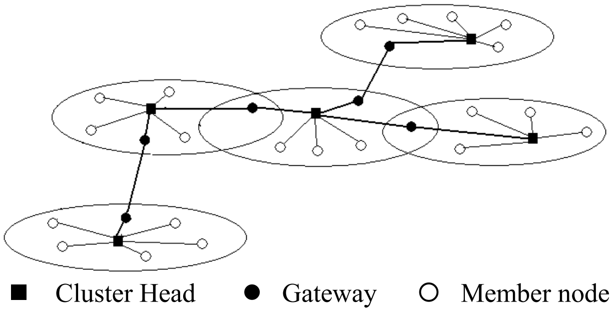

Figure 1. A cluster based ad hoc network [5]

The information about link states (uni-directional or bi-directional) and its neighbors' states (retained by every node in CBRP) are presented in a neighbor table. A cluster head keeps information of its neighboring clusters, in addition to the information of all members in its cluster. The information includes the cluster heads of neighboring clusters and gateway nodes connecting it to neighboring clusters [6].

CBRP proposes the shortening route for performance optimization. Since CBRP uses a source routing scheme, a node gets all information about the route when receiving a packet. Nodes exploit route shortening to choose the most distant neighboring node in a route as next hop to minimize the hop number and adapt to network topology changes.

CBRP has the following features [5]:

- Fully distributed operation.
- Less flooding traffic during the dynamic route discovery process.
- Explicit exploitation of uni-directional links that would otherwise be unused.
- Broken routes could be repaired locally without rediscovery.
- Sub-optimal routes could be shortened as they are used.

In these protocols clusters are introduced to minimize updating overhead during topology change. However, the overhead for maintaining up-to-date information about the whole network's cluster membership and inter-cluster routing information at each and every node in order to route a packet is considerable.

B. Mobile Agent

Mobile agent platform is general-purpose software that enables organization to implement many different applications. Moreover it is an intelligent and autonomous agent that can move through heterogeneous network and interact with nodes.

C. Intrusion Detection System Definition

IDS is based on the fact that a hostile activity will be notably different from that of a legal user. So an IDS is a professional guard system that observes patterns of activity in user accounts and alert a system administrator if anything unusual (intrusion) is detected. IDS system after detection, attempts to possibly prevent such activities that may compromise computer security such as confidentiality, integrity, authentication, non-repudiation and availability.

D. Intrusion detection System Classification

There are several ways to categorize an IDS, which in Fig. 2 has been showed. The first Category is based on data collection mechanism and monitoring activity, either on single-host or on multiple-host within network. The second category is based on the technique of intrusion detection and analysis strategy, which have two main types and one hybrid model. These three broad categories of IDS can be used on host-based (HIDS) and network-based IDS (NIDS) systems. Generally, NIDS uses Misuse-based detection and HIDS uses Anomaly-based detection. Each approach has its strengths and weaknesses; each is complementary to the other [2]. The third category is based on architecture of IDS.

In many simple IDS implementation, several categories are combined in a single device for better efficiency.

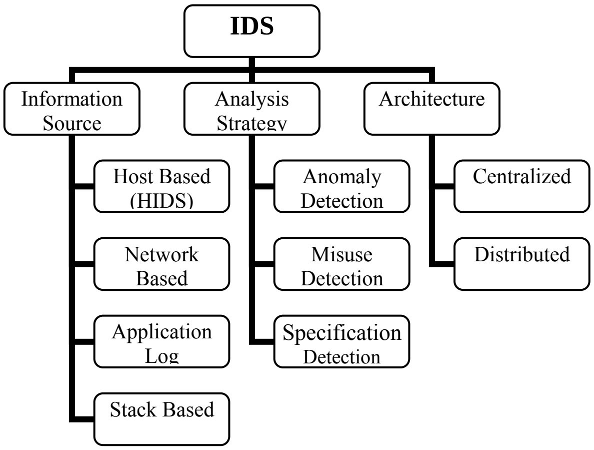

Figure 2. Different IDS classification

E. *Limitation of IDS for MANET*

So far a few researches have been done in intrusion detection for traditional fixed wired networks. However, applying the research of wired networks to wireless networks is not an easy plug-and-play task and the efficiency of IDS solutions that were designed for fixed wired networks are limited for wireless ad hoc networks because of some special properties of wireless ad hoc networks as listed below [7], [8], [9].

- Lack of infrastructure
- Lack of key traffic connection points
- Dynamic network topology
- Operational constrains

To overcome the problem we need to develop a systematic approach for designing the realistic IDS for MANET. Based on these aims the specialized MANET IDS is expected to support several of the following requirements [10]:

- An IDS should use as little system resources as possible to detect and prevent intrusions.
- An IDS should not introduce any weakness and overhead in the MANET.
- An IDS addition of detection should have a proper response.
- An IDS should run continuously and remain transparent to the system and users and have a high accuracy.
- An IDS should be timeliness to perform and propagate its analysis as quickly as possible to prevent the attacker from subverting the audit source or IDS itself.
- An IDS should be fault-tolerant and scalable
- An IDS should be accurate and be able to interoperates with other IDSes as well.

III. Related Works

We classified the works that have been done on security of MANET in the area of IDS into two main categories: *different IDS architecture for MANET* and *security of MANET based on mobile agent.*

According to the system architecture, IDS for MANET security can be classified as Stand-alone, Distributed and Cooperative and Hierarchical IDS [8],[9],[11],[12].

For mobile agents to be useful for intrusion detection, it is necessary that many host and network devices are installed with a mobile agent platform. Contrast this with many expensive IDS schemes that assume every host is installed with a host-based IDS. This new approach (using mobile Agent for IDS in MANET) is not unusual to install a mobile agent in every host especially which has some features that are very useful in MANET [1], [9], [10], [13]-[14]. The followings are the main mobile agent's features that demonstrate straight relevance to the special challenging requirements found in MANET [15]:

- Light-weight
- Conserving bandwidth
- Improving load balancing in the network
- Reducing the total tasks completion time
- Having robust and fault-tolerant behavior

These qualities make mobile agents a choice for security framework in MANET. Table I shows the details of some other researches on IDS, which is based on mobile agent.

IV. Distributed Hierarchical IDS Using Mobile Agents for MANET

Our proposed solution is "Cluster-based Distributed Hierarchical IDS using Mobile Agents" for MANET over CBRP. Fig. 3 shows a simple framework that helps us to propose a cluster-based distributed hierarchical IDS using mobile agents.

In this paper we have chosen CBRP as MANET routing protocol, and based on its certain properties the cluster head can be the best location to add IDS on network, because they can monitor and capture live packet traffic on the network.

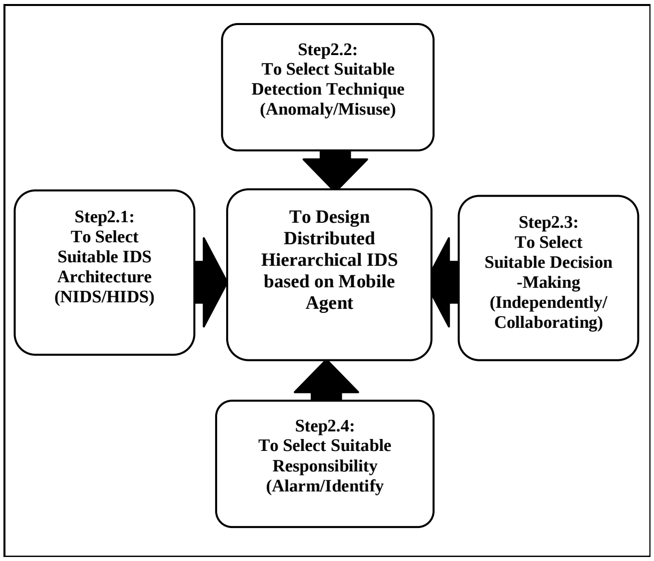

Figure 3. Framework for designing our cluster-based distributed hierarchical IDS using mobile agent

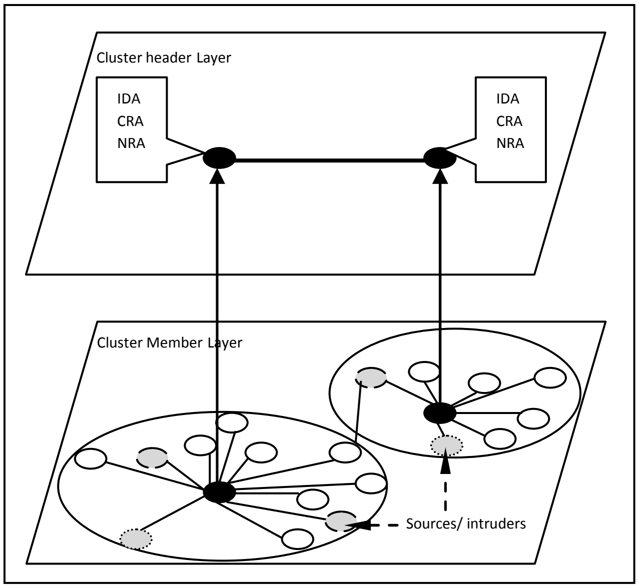

Figure 4. Infrastructure overview of proposed distributed hierarchical IDS

We apply the cluster-based distributed hierarchical IDS model, which uses several mobile agents. This model consists of two layers, cluster member layer and cluster head layer. Fig. 4 shows the infrastructure overview of proposed cluster-based distributed hierarchical IDS using mobile agents.

For the sake of modularity, the task intrusion detection and response have been divided among different agents. The descriptions of the agents are as follow [2]:

1) *Intrusion Detection Agent (IDA):* Intrusion Detection Agent (IDA) is applied on each cluster head, which includes Decision Making Agent (DMA) and Cluster Response Agent (CRA). In fact, in this design we use modified independent decision-making because we have clustering algorithm with cluster head over the network. Cluster head using anomaly detection engine, which has higher detection accuracy compare with the misuse detection, independently analyses and makes decision on the entire information inclusive normal and abnormal situation (intrusion). An IDA is not only able to detect an intrusion, but also can identify the possible attacker and send alarm to all cluster

TABLE I DIFFERENT PROPOSED IDS BASED ON MOBILE AGENT

PROPOSED SYSTEM	BY	METHODOLOGY	ARCHITECTURE	HIGHLIGHTS
IDS Based on a Static Stationary Database (SSD)	Smith (2001)	• Mobile agent-based Anomaly , Misuse & Hybrid detection • Independently decision making	Two parts: • Mobile IDS agent • Stationary secure data	• Mobile agents do intrusion detection by using five parts: ADM, MDM and etc. • The use of SSD limits communication between IDS agents • SSD stored in high physical security area ,but still this is in risk of attack (-) • Periodically up to date with non-mobile database (-)
Local Intrusion Detection System (LIDS)	Albers et al. (2002)	• Mobile Agent-based Distributed Anomaly detection • Independently • Decision making	Two key elements: • Several data collecting agents: o LIDS agent o Mobile agent o MIB agent • A common communication framework	• Use SNMP data located in MIB to process data, transmit SNMP requests to remote hosts to overcome the unreliability of UDP, by using mobile agent (+) • Cost of local information collection is negligible by running SNMP agent on each node (+)
Distributed IDS Using Mobile Agent	Kachirski & Guha (2002)	• Mobile Agent-based Anomaly detection • Modified independently & cooperatively	• Multiple sensor types for specific function: • Network monitoring • Host monitoring • Decision making • Action	• Multiple sensors used to implement a bandwidth-conscious scheme • Distributed IDS make better network performance (+)
A Cooperative IDS Framework	Huang & Lee (2003)	• Cluster -based Anomaly detection, • Independently & Cooperatively	• Special kind of clustering algorithm • Finite State Machine of the cluster-formation protocols	• Cluster-based improves the efficiency of IDS in terms of memory usage & network overhead (+) • Need to prevent a compromised node be elected as cluster head (-) • Not mention false alarm rate (-)

members using piggybacking technique (through the CRA). Piggybacking does not utilize bandwidth and as result it does not add any overhead. We piggyback list of all intruder nodes (from black list) to hello message that periodically is transmitted between cluster head and cluster members. Whenever the intrusion is detected, the IDA can determine that the cluster is under attack and using CRA, a response can be initiated to prevent or minimize damage to the cluster. This response can initiate alarm to other cluster members.

2) *Network Response Agent (NRA):* Each cluster head acts as IDA for its cluster. After each cluster head independently detect and response to intrusion by IDA, NRA will be initialized extra response to other cluster heads if the intruder is a gateway node. Fig. 5 illustrates the cluster head state-diagram as well as cluster member state-diagram of our proposed cluster-based distributed hierarchical IDS.

V. Discussion and Conclusion

As we know, the traditional way of protecting networks with firewalls and encryption is not efficient, because they designed for known attacks and also they create some overhead. Cryptography will not protect against malicious inside nodes and it just protects against some types of attacks from external nodes. IDS tools are capable of differentiating between insider attacks initiating from inside the network and external ones. Unlike firewall that is first line of defense and monitors border nodes to detect the external attacks, IDS appears just after an intrusion has happened and a node or network has been compromised. On the other hand intrusion detection monitors internal attacks as well as external attacks; that is why IDS are called the second line of defense. Main objective of this research was to design an efficient distributed hierarchical IDS using mobile agent for a MANET over CBRP.

As Table II shows sending and receiving packets increase the energy consumption; which is one of the important parameter that we had to consider for designing efficient IDS. However by considering these issues, incorporating cluster-based distributed hierarchical IDS into CBRP using mobile agent would enhance the security of MANET. The unique features of cluster based routing protocol are the main factors of our success in achieving our goal to propose some enhancement based on the characteristics and measure the efficiency of intrusion detection system in term of bandwidth utilization and energy consumption [12]**.**

TABLE II Power Consumption Measurements (send & Receive parameter) for LUCENT IEEE802.11 2MBPS WAVELAN PC CARD 2.4 GHZ

Parameter	µW.sec/byte	µW.sec
Broadcast Send	1.9 * size	+ 266
Broadcast Receive	0.50 * size	+56

The following diagram shows the flow of using cluster-based distributed hierarchical IDS over CBRP. We define a black list for the nodes that sent intrusion packet to network. We define a timer and counter for every node which create and send intrusion packet for manage of control intrusion packet.

We believe that our proposed cluster-based distributed hierarchical IDS using mobile agent will exhibit the

TABLE III Our Expectation from the Proposed Cluster-based Distributed Hierarchical IDS in compared with the Existing IDSes

Proposed system	**Stand-alone / Watchdog & Pathrate**	**Distributed & Cooperative IDS**	**(RIDAN)**	**Local Intrusion Detection System (LIDS)**	**IDS Architecture Based on a Static Stationary Database**	**Distributed IDS Using Mobile Agent**	**A Cooperative IDS Framework**	**Our Proposed / CBDH-IDS[*] based on Mobile Agents**
Provide Weaknesses/ Overhead	No	Yes	Yes	No	Yes	No	No	**No**
light weight	Yes	Yes	Yes	No	No	Yes	Yes	**Yes**
Fault-tolerant	Yes	Yes	Yes	No	No	Yes	Yes	**Yes**
Scalable	Yes	Yes	Yes	Yes	Yes	Yes	Yes	**Yes**
Detects new attacks patterns	Yes	Yes	Yes	Yes	Yes	Yes	Yes	**Yes**
Interoperates with other IDSes	No	No	No	Yes	No	No	No	**Yes**

[*] CBDH-IDS: Cluster-Based Distributed Hierarchical Intrusion Detection System

development of security in wireless ad hoc networks. Furthermore, adding cluster-based distributed hierarchical IDS to MANET does not increase the communication message overhead as well as energy consumption due to unique features of CBRP for managing communication message.

We expected that our proposed cluster-based distributed hierarchical IDS provides some enhancement in compared with the previous IDS models, that is listed in Table III.

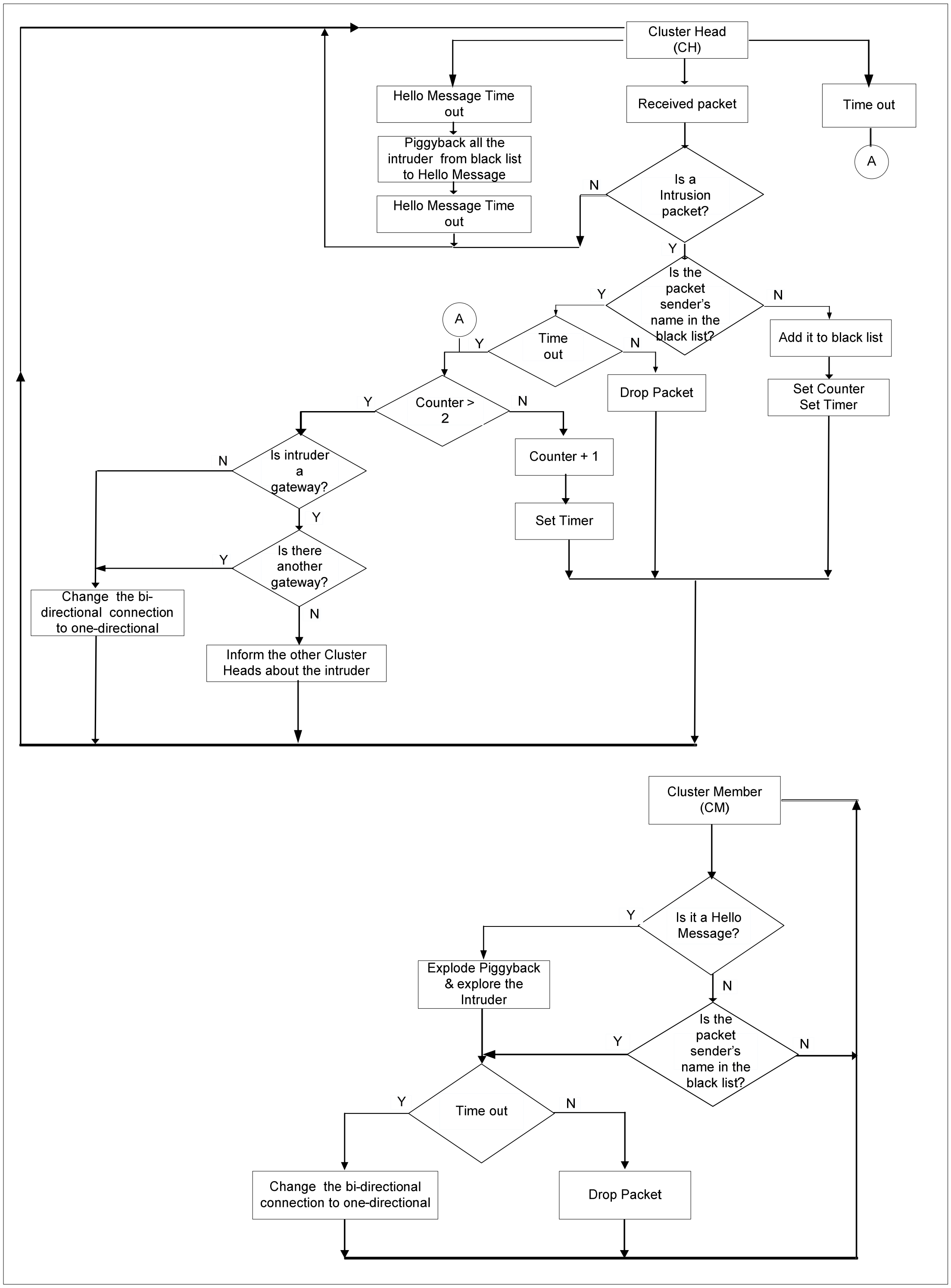
Cluster Head (CH)
Hello Message Time out
Received packet
Time out
A
Piggyback all the intruder from black list to Hello Message
Hello Message Time out
N
Is a Intrusion packet?
Y
Is the packet sender's name in the black list?
Y
N
A
Time out
Y
N
Add it to black list
Drop Packet
Set Counter Set Timer
Y
Counter > 2
N
Counter + 1
Set Timer
N
Is intruder a gateway?
Y
Y
Is there another gateway?
N
Change the bi-directional connection to one-directional
Inform the other Cluster Heads about the intruder
Cluster Member (CM)
Y
Is it a Hello Message?
N
Explode Piggyback & explore the Intruder
Y
Is the packet sender's name in the black list?
N
Y
Time out
N
Change the bi-directional connection to one-directional
Drop Packet

Figure 5. Flow of using cluster-based distributed hierarchical IDS in cluster heads and cluster member

Acknowledgment

Our thanks to the Universiti Sains Malaysia for the fellowship and research grant as well as to NAv6 members who help us with the time off for the network engineering discourse.

References

[1] The National Institute of Standards and Technology.ANTDwebmaster.May,2001 . Mobile ad hoc network. Available: http://w3.antd.nist.gov

[2] B. Pahlevanzadeh and A. Samsudin, 2007. Distributed Hierarchical IDS for MANET over AODV+. *Proceedings of the 2007 IEEE International Conference on Telecommunications and Malaysia International Conference on Communications,* 14-17 May 2007, Penang, Malaysia.
[3] A. Hamidian, "A Study of Internet Connectivity for Mobile Ad Hoc Networks in NS 2" , Master's thesis, Lund Institute of Technology, Sweden, January 2003, Available: http://www.telecom.lth.se/Personal/alexh/rapport.pdf

[4] Mehran Abolhasan , Tadeusz Wysocki , Eryk Dutkiewicz Changling Liu, Jörg Kaiser, A review of routing protocols for mobile ad hoc networks Ad hoc networks, 2004, pp. 1-22.

[5] Seyed Amin Hosseini Seno, Bahareh Pahlevanzadeh, Tat-Chee Wan, Rahmat Budiarto, Masoumaeh Ghahremani, "A New Approach CBRP Based Resource Information Management in MANETs," *International Journal of Computer Science and Network Security, (IJCSNS),* Vol. 8 No. 5, May 30, 2008, pp. 301-308.

[6] Mingliang Jiang, Jinyang Li, Y.C. Tay**,** INTERNET-DRAFT draft-ietf-manet-cbrp-spec-01.txt, National University of Singapore, July 1999. Latest access Jun 2008 at URL: http://www3.tools.ietf.org/wg/manet /draft-ietf-manet-cbrp-spec/draft-ietf-manet-cbrp-spec-01-from-00.diff.html.

[7] P. Brutch, and C. Ko, "Challenges in intrusion detection for wireless ad-hoc networks," *Applications and the Internet Workshops*, 2003, pp. 368─373.

[8] L. Stamouli, P.G. Argyroudis, and H. Tewari, "Real-time Intrusion Detection for Ad hoc Networks," Proceedings of *sixth IEEE International Symposium Computers and Communications,* June 2005, *pp.374 ─38*0.

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

[10] A. Mishra, K. Nadkarni, and A. Patcha, "Intrusion detection in wireless ad hoc networks," Proceedings of *IEEE Personal Communications.* Vol. 11, 2004, pp. 48─60.

[11] Y. Zhang, and W. Lee, "Intrusion Detection in Wireless Ad Hoc Networks," Proceedings of *the Sixth Annual International Conference on Mobile Computing and Networking (MobiCom 2000)*, 2000.

[12] Laura Marie Feeney, Martin Nilsson: "Investigating the Energy Consumption of a Wireless Network Interface in an Ad Hoc Networking Environment". INFOCOM 2001: 1548-1557.

[13] O. Kachirski, and R. Guha, "Intrusion Detection Using Mobile Agents in Wireless Ad Hoc Networks". Proceedings of *the IEEE Workshop on Knowledge Media Networking,*2002, pp.153─158.

[14] Y. Huang, and W. Lee, A Cooperative Intrusion Detection System For Ad hoc Networks. *In Proceedings of the 3th international conference on Distributed Computing systems,* vol 6, *2004*, pp. *1155─1168.*

[15] A. Hijazi, and N. Nasser, "Wireless Using mobile agents for intrusion detection in wireless ad hoc networks," Published *Second IFIP International Conference on March 2005*, pp. 362─366.