Policy Based Danger Management in Artificial Immune System Inspired Secure Routing in Wireless Mesh Networks

Mahira Atham Lebbe (Mahira M Mowjoon), Johnson I Agbinya and Zenon Chaczko

***Abstract*— This paper introduces Policy based Management Information Base to mange danger in Artificial Immune System inspired secure routing in Wireless Mesh Networks. WMN management functions are defined and the paper focuses only on the security function. Proposed policy based management and typical operation of the architecture are also reported.**

***Index Terms*— Artificial Immune System (AIS), Management Information Base (MIB), Wireless Mesh Networks (WMNs)**

I. Introduction to Wireless Mesh Networks (WMNs)

Wireless Mesh Networks (WMNs) have recently gained mounting curiosity and have emerged as a promising technology with great budding for a large array of applications such as real time transportation systems, disaster networking, rural networks, health and medical systems, building automation and security surveillance systems. WMNs are self organizing and self configuring wireless networks implemented with IEEE 802.11 hardware. The value of a network is perceived by the services it provides to its users. Unfortunately, security is often a secondary consideration and some what contradictory to usability. Consequently, many networks are inadequately safeguarded against a variety of attacks. Wireless networks are more vulnerable than wired networks because the wireless medium is shared and accessible through the air. Unfortunately, WMNs presents additional security challenges due to their decentralized nature, dynamic network topology and easy access to the radio medium. Hence security is an important consideration for the practical operation of WMNs. Inside security, secure routing is imperative and the problem of routing in WMNs is to be urgently investigated in order for the successful deployment of these networks.

II. Architecture of WMN

According to the 802.11s standard, nodes in a mesh network fall into 4 categories; Client or Station (STA) is a node that requests services but does not forward frames, nor participate in path discovery, Mesh Point (MP) is a node that participates in the formation operations of the mesh, Mesh Access Point (MAP) is a MP attached to an access point (AP) to provide services for clients (STA) and Mesh Portal Point (MPP) is a MP with additional functionality to act as a gateway between the mesh and an external network like the Internet. Fig.1 shows the architecture according to 802.11s standard.

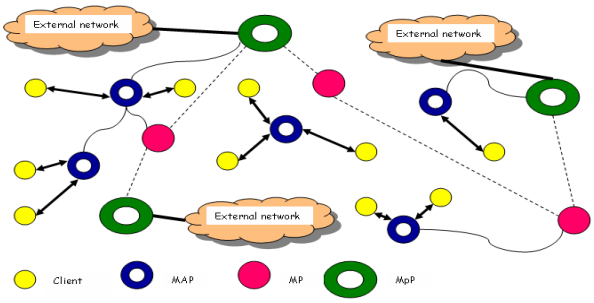

Figure1: WMN Architecture

III. Secure routing in WMNs

In our previous work [1], we proposed Human Immune System (HIS) concept, subsequently Artificial Immune System (AIS) Models to embed in secure routing in WMNs. The selected AIS model among other models in the literature is the “Danger Model”. In order to apply HIS concepts in WMNs, we have mapped HIS elements with WMN components. The table below shows the mapping between HIS and WMN [1].

Table I: Mapping HIS with WMN

HIS	WMN
Body	The entire WMN
Self-Cells	Well behaved network resource nodes
Non-Self Cells	Corrupted or well-behaving but unauthorized nodes inside the network or any external input either friendly or malicious
Antigen	Possible cause of interruption or danger to the network
Antibody	Recovery or protection actions for the node in danger against antigen

Manuscript received January 11, 2008.

Mahira Atham Lebbe (Mahira M Mowjoon), Doctoral Researcher, Centre for Real-time Information Networks, Faculty of Engineering, University of Technology, Sydney, Australia; e-mail: mathamle@eng.uts.edu.au.

Johnson I Agbinya, Senior Lecturer, Centre for Real-time Information Networks, Faculty of Engineering, University of Technology, Sydney, Australia; e-mail: agbinya@eng.uts.edu.au.

Zenon Chaczko, Senior Lecturer, Centre for Real-time Information Networks, Faculty of Engineering, University of Technology, Sydney, Australia; e-mail: zenon@eng.uts.edu.au

The process of modeling WMN security based on danger theory consists of two steps [1]. The first step is to recognize the danger signal and the second step is to classify danger signals into different levels. Danger signals can therefore be issued by the network cells (nodes). The danger signals signify the state of the mesh network. Some examples of danger signals are the number of error messages generated per second by a broken link of the network, the number of transmitted packets per second, congestion over a threshold, inappropriate disk activity, node failure, noise and viruses. In order to realize the first step, we need to find a mechanism to store the state information of the network elements. In this paper we propose a method to store node state information in the network. In our proposal, we basically introduce object oriented approach. The WMN entities are treated as objects and each object has a unique ID, attributes and behaviors.

IV. Wireless Mesh Network Management Functions

In this section we define five major management functions and concentrate on security management, specifically AIS embedded secure routing.

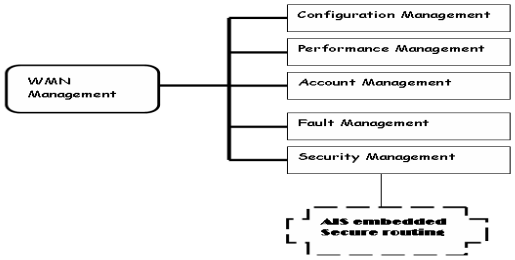

Figure2: WMN Management functions

The Configuration Management records and maintains network configuration, parameter updating for ensuring correct network operation; Performance Management includes performance measurement of hardware and software. For example, how long a request takes to give a response? How many responses are given to a request?; Accounting Management handles network users. For instance, how many times a user logs into the system? Or how many requests are done each time; Fault Management finds problems or errors from network. This is used to know if a network component was running or not and Security Management is responsible for controlling the process of information access in the network, providing protection for network resources, services and data to avoid danger. During this process the system may check if a user can log in the system or not.

V. Management Information base (MIB)

A MIB is a tree data structure, where the leaves are individual items of data called objects or variables. A MIB object may be, for example, a counter or a protocol status. These managed objects allow remote monitoring and control of systems over a network. The frequent incorrect way to visualize a MIB is as a database on a managed system. It is more correct to view a MIB as definitions of the information that can be accessed and the events that can be reported by standard protocols. Standard operations are requested or performed on a system via a management agent by management clients. It is the responsibility of the management agent to access the requested information and return it to the requesting client. Some example values for MIB object are [3] Object type which identifies the type of MIB object, Syntax which identifies the data type which models the object, Access which identifies the maximum level of access, Status which specifies the status of a managed object and a description which provides a textual description of the managed object. In wireless networks SNMP MIBs are used to manage hardware.

The SNMP MIB is conceptually a tree structure with conceptual tables containing information such as transmission medium or routing protocols. MIBs may be standard or enterprise. Internet standard MIBs are defined by working groups of the Internet Engineering Task Force (IETF) and published as Requests for Comment (RFCs). Enterprise MIBs are defined by other organizations, usually individual companies.

The definition of managed objects may progress independent of the protocols used to operate on the MIB and the MIBs can be reformatted accordingly. However, operations may be generalized into three categories: information retrieval, information modification, and unsolicited information reporting.

VI. Policy based MIB

The increasing complexity and heterogeneity of WMN initiates major challenge to network management. Thus, good management policies are critical for successful operation of WMN. Policy based management supports the network and service administrators by (a) using a high degree of viewpoints of quality and (b) providing a variety of the services while decreasing the cost of running the services [2]. It is an appropriate means to automate many of the management functions. In policy based management systems, since the policies defined by the administrators do not directly translate into device configurations, the system uses the current network state and configuration to determine a set of configurations that enforce these policies [2].

We propose the following four issues to sense in order to ensure the successful deployment of policy-based management in WMN:

- What kind of management knowledge is needed to uphold the formation of the policy?
- How to choose the apposite network states which form the management knowledge
- How to apply the composed knowledge for a safe policy application
- How can the policies specified be imposed efficiently? i.e. the requested network service should be offered without adversely affecting other services and the quality of the requested services

VII. Proposed Architecture of the policy based management system

The proposed architecture consists of three major components, policy based MIB (PMIB), Policy Management

System (PMS) and the complete WMN. Policy Storage (PS), Network state information (NS) and Action formation Unit (AU) shape the PMIB; Monitoring Unit (MU), Policy forming Unit (PU) and predefined algorithm (AL) form PMS; and WMN consists of all elements defined in section II. The figure below shows the proposed architecture.

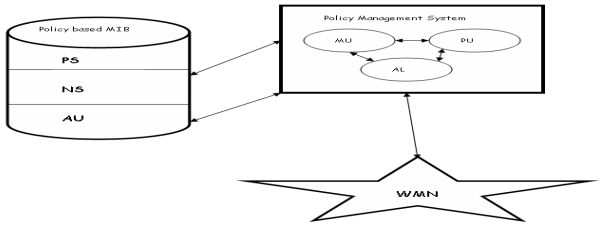

Figure3: PMIB Architecture

- Monitoring Unit (MU): Monitors and receive network state information
- Policy forming Unit (PU): Compose policies
- Predefined algorithm (AL): Assists in forming policies
- Policy Storage (PS): Accumulate composed policies
- Network state information (NS): Provide network state information in timely manner
- Action formation Unit (AU): Initiate network actions according to the policies

VIII. Basic Operation of the Architecture

Based on the received network state information, policies are produced. Then policy check request is initiated and sent to PMIB. Based on the decision, action to perform is sent to PMS. Then PMS instruct WMN accordingly.

IX. Typical Operation of the Proposed Policy Based Management

The operation runs on the following algorithm

Start

Receive state information of the network devices

Form policy / policies according to a predefined algorithm

Accumulate formed policy / policies into the Policy Management System (PMS)

Policy management system queries the policy based MIB automatically

Check composed policy (policies) is not creating unreachable or conflict policies

If reachable and not conflicting

PMS convert new configuration into realizable policies

Save updated / new policy in policy based MIB (PMIB)

Send policies/policy to relevant devices

Activate network accordingly

Else

Record the state information for future prediction

Endif

When policy requested by the network device / devices

Network device initiate request to PMS

PMS process the request

Send appropriate signals to network elements

Network reacts accordingly

End

X. Future Work

We are scheduling to improve proposed policy based management algorithm in our next paper and implement our novel idea in real world applications. Also we will focus on the second step in the process of modeling WMN security based on danger theory introduced in our previous paper [1].

References

[1] Mahira Atham Lebbe, Johnson I Agbinya, Zenon Chaczko and Frank Chiang, Self-Organized Classification of Dangers for Secure Wireless Mesh Networks, ATNAC2007

[2] Generalized Policy Framework Architecture, Work in Progress, **<draft-blight-gen-poli-arch-OO.txt>**

[3] http://www.cisco.com/en/US/docs/voice_ip_comm/pgw/7/mibs/guide/7MIB_Ch1.html

[4] [4] M.Sloman, E.Lupu, Policy Specification for Programmable Networks, in proceedings of First International Working Conference on Active Networks (IWAN'99), Berlin, June 1999

[5] [5] F. GAO, X. Ye, J. Gutierrez, Enhancing MIB Functionality to Cater for Interoperability in Network and Systems Management, in proceedings of APNOMS'99, Kyoungiu, Korea