A Co-Operative Intrusion Detection System in Mobile Ad-Hoc Network

S.S.Chopade
Dept. of Electronics & Telecommunication
SSPACE, Wardha, M.S, India

Prof.N.N.Mhala
H.O.D. of Electronics
Engg.Bapurao Deshmukh COE
Sevagram, Wardha, M.S, India

ABSTRACT
Mobile ad-hoc networking has become an exciting and important technology in recent year because of the rapid proliferation of wireless devices. The security of data becomes more important with the increased use of commercial application over wireless network environments; there were several problems of security in wireless networks due to different types of attack and intruders. There were better methods an intruding handling procedure available for fixed networks. But it was difficult to analyze attacks in the mobile ad-hoc environments. The reason is that there is no central point to control all the activities in the network and dynamically changing network topology and behavior and limited power level of mobile devices. Attacks by intruders cause unauthorized use of wireless network so that the whole network will be suffered from packet loses. We are introducing three types of internal attack named as Node isolation, route disruption, Resource consumption; we presented an approach to handle such type of internal attacks for wireless network. We report our progress in developing intrusion detection capabilities for MANET. The proposed work can be performed by modifying ad-hoc on demand distance vector routing protocol. The simulation experiments are conducted on NS-2 environment in Linux platform.

Keywords: MANET, attacks, Node isolation, Route disruption, Resource consumption

1. INTRODUCTION
In recent years, with the rapid enhancement of wireless devices e.g. mobile laptops, computers, PDA and wireless telephone, the potential and importance of mobile ad-hoc networking has become apparent. Basically ad-hoc networks are temporary in nature. It usually has a group of stations communicating with each other and can be formed spontaneously. A MANET is an autonomous system of mobile nodes connected by wireless links. Each node operates not only as an end system but as a router also to forward packets. The MANET does not require any fix infrastructure such as base station. Therefore, it is an attractive networking option for connecting mobile devices quickly. The existent protocol, application and services assume that MANET is a cooperative and friendly network environment and do not accommodate security. Therefore, the number of attacks in this is more and we aim to address the problem of attacks. Intrusion detection techniques are widely used in wired network to protect the systems. But this IDS can not directly applied to wireless Network because in Ad-hoc network it met a lot of problem i.e. there is no central point to control all the activities, dynamically changing network topology, limited power level of mobile devices. Hence there is a need for efficient wireless network technology to provide safe network. The basic requirement for IDS to be implemented in adhoc network is the IDS should not introduce a new weakness in the MANET. Our basic aim is IDS should run continuously and remain transparent to the system, an IDS should not only detect but also respond to detected intrusions preferably without human intervention and most important IDS should use as little system resources as possible. The proposed wireless intrusion detection system has been simulated using ns-2 environmental in Linux platform

2. RELATED WORK

A lot of work has been done in the past on intrusion detection system by various researchers.
Macro Domanico Aime [1] proposed a distributing Intrusion Detection System in which each mode monitors the traffic flow on the network and collects relevant statistic about it.

Yian Huang [2] developed intrusion detection capabilities for MANET. He investigated how to improve the anomaly detection approach to provide more details on attack types and sources. He addressed the run time resource constraint problem using a cluster base detection scheme where periodically a node is elected as the ID agent for a cluster. This experiment conducted using the ns-2 and Mob Emu environments

Peter Baroon, Stefan Weber, Siobhan Clarke, Cahiil [3] built a wireless ad-hoc network for Dublin. The network provides a large scale tested of application for protocols for mobile ad-hoc networks

Nils Aschenbruck [4] researched a project called MITE which funded by German armed forces. A distributed intrusion detection system for tactical MANETS has been developed.

Nachiket R. Potlapally's work [5] focuses on one important constraint of several devices battery life and examines how it is impacted by the use for various security mechanism. He has studied the energy consumption requirement of the most popular transport -layer security protocol; secure socket layers. (SSL)

Yu-Xi Lim, [6] member from IEEE studies an off the shelf wireless access point was modified by downloading a new lines operating system with non-standard wireless access point functionality in order to implement a wireless intrusion detection system that has the ability to actively respond to identified threats. Increasing no of organizations are deploying wireless networks, mostly utilizing the IEEE 802.11 b protocol.

J. P. Anderson [7] did the work on computer security threat monitoring and surveillance. Technical report, James P. Anderson Company, Fort Washington, Pennsylvania.

S. Basagni. [8] Distributed clustering for ad hoc networks. In ISPAN-99, International Symposium on Parallel Architectures, Algorithms, and Networks

S. Basagni, K. Herrin, D. Bruschi, and E. Rosti [9] Secured pebble nets in Proceedings of the 2001 ACM

3. INTRUSION DETECTION SYSTEM DISCPRIPTION

Intrusion detection is the process of identifying and responding to malicious activity targeted at computing and networking resources. Intrusion detection systems are widely used in wire network to protect network system. This intrusion detection techniques can not applied directly to wireless network. However, this wireless network has some disadvantages e.g. nodes roaming freely in a hostile environment with relatively poor physical protection. Hence there is a need to consider malicious attacks not only from outside but also from within the network from compromised nodes. Eaves dropping might give an attacker access to secret information thus violating confidentiality a. active attacks could range from deleting data, injecting wrong messages impersonate node, etc. it exposes a risk that other users can share the same channel and misuse it. So there is a problem of security in wireless network. Hence, there is a need for efficient wireless network technology to provide safe network accesses to users and also the efficient wireless intrusion detection system that not only detects different possible attack but also to recover from them.

This section gives an overview of intrusion detection system-The main design goal is:

1) To identify various possible attacks in wireless network system and

2) To propose a method for detecting attacks in MANET.

This work can be performed by modifying ad-hoc on demand distant vector protocol.

The proposed work can be divided into three modules, based on packet transfer under normal and attack mode. The intruder which has been detected in the detection phase should be isolated from the network in the recovery phase. The intruder has no action network environment since it has been isolated as the individual victim. Now, the network is free from the action of intruder and thus results in the secure communication. The overall system architecture has been shown in figure (1).

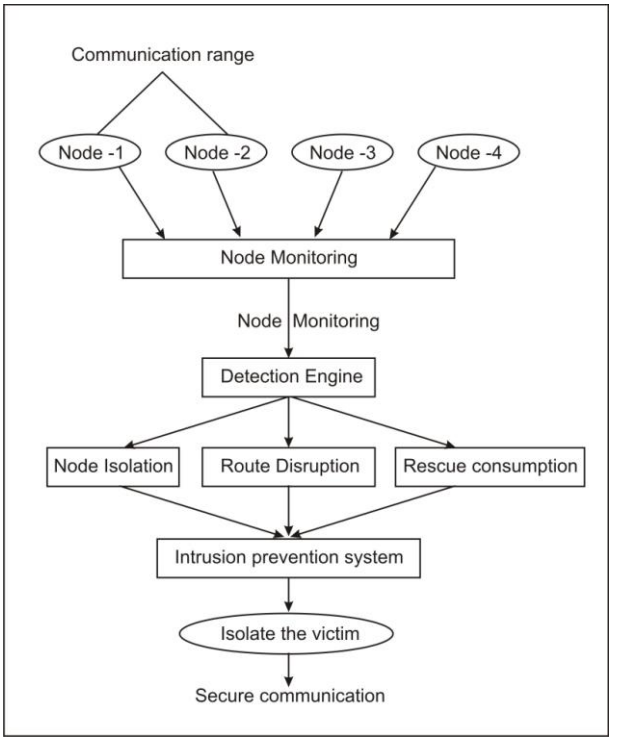

Fig. System Design

The overall system design includes different nodes. Each node can communicate with each other randomly and also based on communication range. The transfer of packets among different nodes could be easily visualized under the simulation environment. For each traffic flow a source/destination pair is randomly selected from the node set. Every nodes can move arbitrarily, the network topology from time to time at the communication links between mobile nodes break frequently.

The Table1 below shows the parameter as an example:

Parameters	**Value**
Simulation duration	100 sec
Topology	1000m* 1000m
Number of mobile Nodes	20
Transmission range	250m
Node movement model	Random way point model
Traffic type	CBR(UDP)
Data payload	512 bytes

4. PERFORMANCE ANALYSIS

We use NS-2.29 to study this experiment. . Network simulator is a discrete event simulator developed at UC Berkley in C++ and Otcl. The simulator includes protocol implementation for most network components. It can simulate UDP, TCP agent, it can generate application traffic like CBR,

and VBR.NS-2 has two components C++ implementation of various network components and TCL scripts uses to access those classes. NS is a Otcl interpreter with network simulation object libraries. Otcl scripts uses objects from these libraries to create overlay of a network.

The important property of a mobile ad-hoc network is a dynamic network topology. Every node can move arbitrarily, the network topology changes from time-to-time and the communication links between mobile nodes break frequently. At the time simulation each node randomly selects a destination in the network and move towards a destination at a speed that is randomly selected from the range. [0, max Speed], where speed max represents node max moment speed. By adjusting the values of max speed and pause time, different network topology can be simulated. The reduction in packet size could be easily understood which exactly shows the action for route disruption attacker over the system. in resource consumption attacks, an attacker tries to consume more network that need than or storage space. In this attack the particular node consumes more bandwidth also occupies more storage spaces without providing them to the other nodes The results calculated for packets drop in this attacks.

5. EXPERIMENTAL STUDIES

We have conducted the following experiment using ns2.29 simulator on Fedora 9 in order to study the different types of internal attacks & their Intrusion Detection System.

5.1 PARAMETER SELECTION

We are to apply the **random way-point** model to emulate node mobility patterns with a topology of **500m by 500m**. We use both **TCP** and **UDP/CBR** as underlying transport protocol. The maximum number of mobile nodes is set to be **8.** Transmission range is **1.5m.** All trace have a run time of **100sec.** some regarding simulation environment given in tables.

An important property of a mobile ad-hoc network is dynamic network topology. Since every node can move arbitrarily. Network topology changes time to time and the communication links between mobile nodes break frequently. This simulation parameters is shown in Table2

Table2: **Simulation parameters**

Parameters	**Value**
Simulation duration	100 sec
Topology	500m* 500m
Number of mobile	08
Nodes	1.5m
Transmission range	Random way point model
Node movement model	CBR(UDP)
Traffic type	50 bytes
Data payload	

Under Simulated environments, the three different attacks have been introduced and their corresponding action in the network topology with packet loss is predicted in the following section.

5.2 SIMULATED ATTACK

RESOURCE CONSUMPTION (RC) attacks

In resource consumption, an attacker might try to initiate large number of route requested to bogus destination in order to exhaust the resources of the network. Selective dropping of packet resulting in increased number of route requests from neighbor nodes that have
limited routing capabilities. The result calculated for packet drop is as shown in table 3.

Under the normal mode, main node transmits 3000 packets to node3. Node 1 acts as resource consumption attacker. At the same time node 5 also acts as a malicious node. Under attack mode 30000 packets are dropped from node 1. Actually it consumes that much amount of packet under attack mode due to the action of attacker rather to be 3000 as in normal mode. As a result, a huge amount of resource consumed. Thus the resource consumption attack, over the network nodes, is predicted. This attack is introduced at 30 sec.

NODE ISOLATION (NI) ATTACK

The action of node isolation attack is preventing a node from communicating with other node. Under this attack node gets isolated from the network topology due to action of attacker over the system. In our simulation experiment node0 send 3000packets towards the destination i.e. node3 but node 4 acts as an attacker and it isolates node 0. Under attack mode 16000packets are dropped. This clearly distinguishes the action of attacker. This attack starts at the moment of 50^{th} sec.

ROUTE DISRUPTION (RD) ATTACK

The action of route disruption is breaking of an existing root or preventing a new route from being established. In this attack under normal mode, node 5 transmits 3000 packets towards destination that is node 6, but node 7 tries to take message from node 5 and drops a number of packets. Under this attack, due to dropping of an existing route, dropping of packets occurs. Here, the result shows 3000packets are sent under normal mode while under attack mode 19000 packets are sent, which clearly distinguish the action of attacker from that normal mode. This attack starts at the moment of 65th sec.

Under simulated environment, these three different attacks have been introduced & the result is shown in table3

Table 3

Name of attack	Packets Under normal mode	Packet drop Under attack mode
RC attack	3000packets	30000packets
NI attack	3000packets	16000packets
RD attack	3000packets	19000packets

5.3 INTRUSIONS DETECTION SYSTEM

In the prevention system, the node which has been identified as an attacker should be isolated from the network environment. In the RC attack node 1 drops a maximum number of packets. This node disrupts the existing route of packet transfer from node 0 to node 4.so node 1 isolated from the network topology at 35th sec.

In the node isolation type attack node 4 acts as an attacker and it isolates node 0 and disrupts the route and drops the number of packets. Therefore. At 55sec node4 is also isolated from the system.

In the Route dispersion attack node 7 acts as a attacker so at 70sec this node is also isolated from the system. After 70 seconds all nodes which act as attackers will be isolated from the system. After the intruder is isolated from the network topology, the safer communication is possible between node 5 and node 6 and the packet loss is reduced.

6. EXPERIMENTAL RESULT

In this section, we will see some few simulation scenarios to understand these network internal attacks in detail.

NAM is tool with ns-2.It gives us a graphical representation of the network and packet traversing through the network. It helps to have cursory glance and deduce some events happening in the simulation. Figure 1 shows graphical representation of 20 mobile node where adjacent nodes are in range to one another.

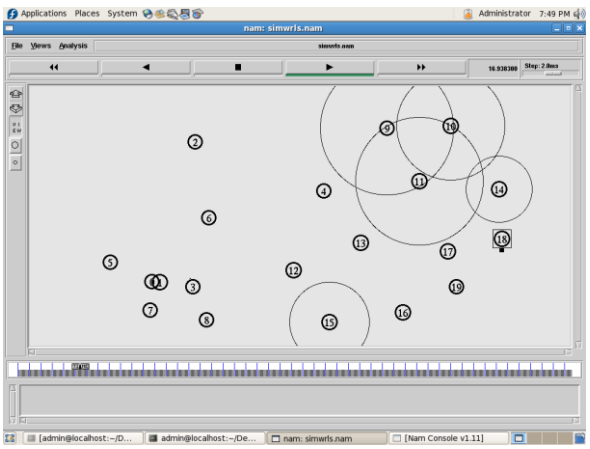

Figure 1: 20 nodes simulation setup

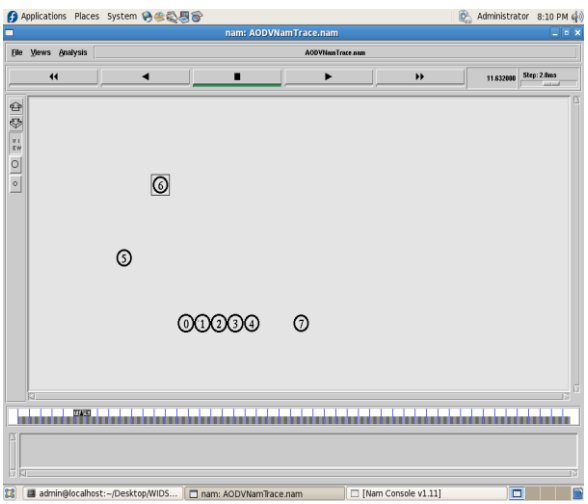

Figure 2: 8 nodes simulation setup

Figures 2 shows the simulation result of 8 mobile nodes .Topology size is 500*500. Nodes positioned in the network environment are monitored by simulation set up. Each node sends packet, based on the communication range and node connectivity.

Figure3: Simulation setup of resource consumption attack

Fig.3 shows simulation set up of resource consumption attack. The connection details are:

- Node 0 to Node 3
- Node 5 to Node 6

Resource consumption attack starts at 30sec node 0, node 1, node 2, and node 5 act as attackers and continuously drops the packets.

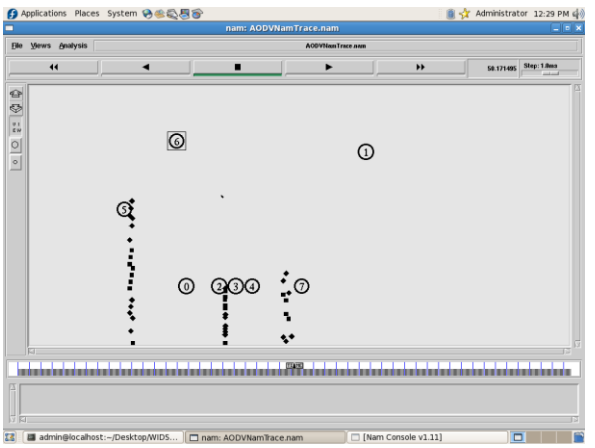

Figure4: Simulation setup of Node isolation attack

Fig.4 shows the simulation set up of NI attack .The connection details are**:**

- Node 0 to Node 3
- Node 5 to Node 6

But due to NI attack node 4 which acts as a attacker isolate node1 from communicating with node 3.This attack starts at the moment of 50th sec.

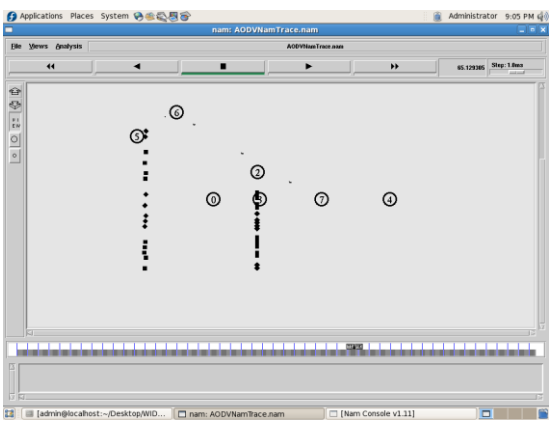

Figure5: Simulation setup of routing disruption attack

Fig.5 shows the simulation setup of RD attack. The connection details are:

- Node 5 to Node 6

In the above result node 7 acts as a attacker and disturbs the main route which is from node 5 to node 6 .This attack starts at the moment of 65th sec.

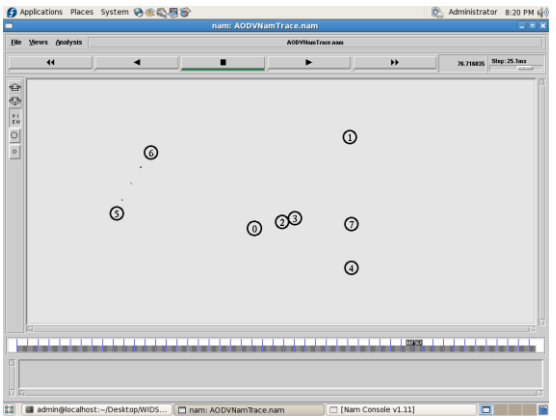

Figure 6: Simulation set up of an IDS System

Fig.6 shows the setup of an IDS system. The node that highly drops the packet, the node which disrupts the existing route and the one which consumes more packets are generally said to be attacker. These nodes are pointed as attacker in the simulation environment and isolated from the topology and

In the above fig at 70sec IDS remove all the attacker from topology so that we get the safe communication between node 5 and node 6.

Final tool that can be helpful in analyzing data from NS-2 is x-graph

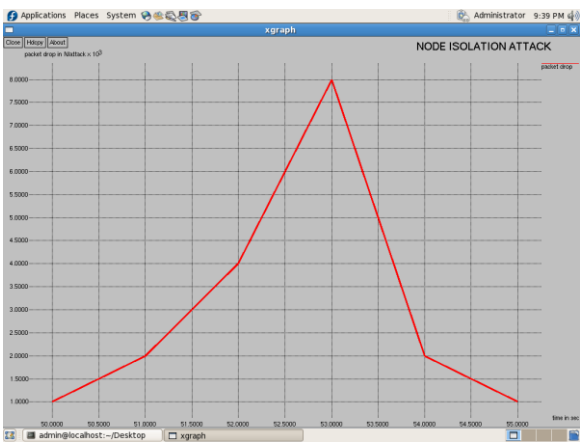

Figure 7: X-graph of NI attack

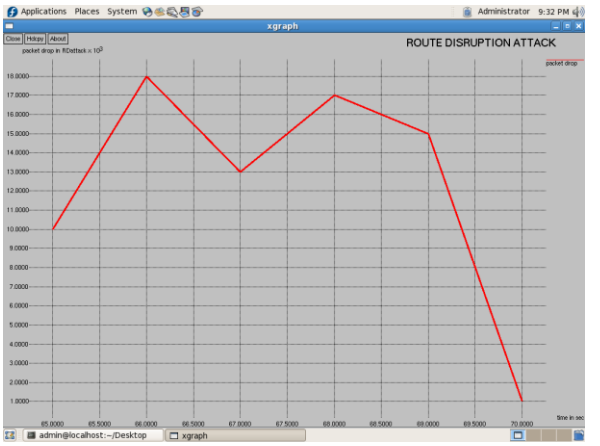

Figure 8: X-graph of RD attack

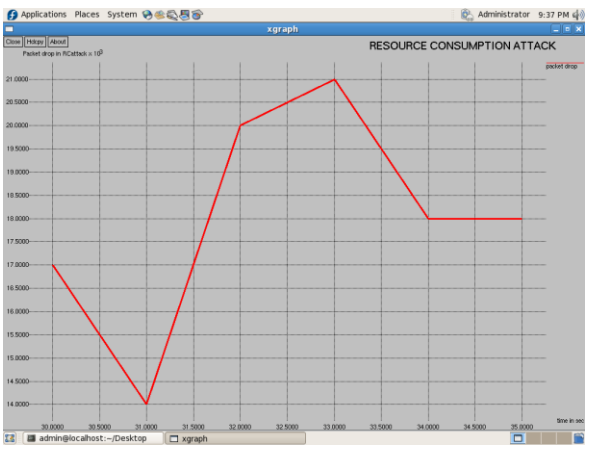

Figure 9: X-graph of RC attack

Hear in fig.7, 8, 9 Red line shows the lost of packets at different time.

7. CONCLUSION

An approach for detecting and analyzing various attacks on MANET has been studied and performance is analyzed. In this paper the basic observation related in intrusion detection system has been studied for the particular node dropping the packets, diverting the route and consuming more resources detected by the proposed systems. Consequently, the recovery procedure has also been discussed for the MANET under various attacks. The recovery has been provided by finding the attacker node and isolating that particular node from the network topology.

In the future enhancement ,simulation can be performed for some complicated attack, also the action of attack can be reduced by using some sophisticated algorithmic techniques, so as the future work ,the recovery phase can be more concentrated.

8. REFERENCES

[1] "An Approach for detecting attacks in mobile adhoc networks"by V.Madhu Viswanatham and A.A.Chari,AP,India

[2] Yi-an Huang, Wenke Lee, "A Cooperative Intrusion Detection System for Ad Hoc Networks", in Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks (SASN), Fairfax, Virginia, October 31, 2003.

[3] Kashan Samad, Ejaz Ahmed, Waqar Mahmood, "Simplified Clustering Scheme for Intrusion Detection in Mobile Ad Hoc Networks", 13th International Conference on Software, Telecommunications and Computer Networks (SoftCOM), Split, Croatia, September 15-17, 2005.

[4] J. Wright, "Layer 2 Analysis of WLAN Discovery Applications for Intrusion Detection 2002 Nov 8 (Online Document)

[5] A Co-operative Intrusion detection system for Ad-hoc Network' Peter Barron @ cs, tcd–ie, Stetan Weber, Siobhan Karke, and Vuinny Cahill. "Experiences Deploying an Ad-hoc Network in an Urban Environment" Stetan Weber

[6] Yu-xi Lim, Tim Shemoyes, proceeding of the 2003 IEEE workshop on Information Assurance, Wireless Intrusion Detection and Response Intrusion Detection in Tactical Multi- Hop Networks' by Nils Aschenbrack, Marko Jahnke University of Bonn, Institute of Computer Sciences IV Roemerstr, 164, Germany (aschenbrack@cs.ani-bo, nnde)) 802,11ninja "802,11ninja.net," available http://802.11ninja.net

[7] Air Defense Inc, "Wireless LAN Security for the Enterprise" Air Defense. Available http://airdefense.net e Air Magnet, "Air Magnet" on 2003 jan 30 Available at http://www.airmagnet.net/11) Finisar "Surveyor Wireless" Finisar, cited 2003 jan 30 Available at: http://goninisar.com/index.html.

[8] Black Alchemy Enterprises, "Black Alchemy Weapons Lab: Fake AP", Black Alchemy Enterprises. Cited 2003 Jan 30) Available at: http://blackalchemy.to/projects/fakeap/fake-ap.html

[9] J.L.DeBoer, "Digital Matrix – AirSnare," Digital Matrix. [online document] [cited 2003 Jan30 available at http://home.arrbi.com/~digital matrix/airsnare/

[10] S Barber. J. Chung, D. Dimdon, D. Lopes, B. McClintock, and D. Wang, "OpenAp," [cited 2003 Jan30availableat HTTP:http://opensource.instant802.com/

[11] J. P. Anderson. Computer security threat monitoring and surveillance. Technical report, James P. Anderson Company, Fort Washington, Pennsylvania, April 1980.

[12] S. Basagni. Distributed clustering for ad hoc networks. In ISPAN-99, International Symposium on Parallel Architectures, Algorithms, and Networks, pages parth, Western Australia, June 1999.

[13] S. Basagni, K. Herrin, D. Bruschi, and E. Rosti. Secure pebblenets. In Proceedings of the 2001 ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc 2001), Long Beach, CA, October 2001.