Secured and Optimized Energy Efficient Routing Protocol to detect Black hole attack in Wireless Sensor Network

Panam R. Fadia
Master Engineering in Information Technology,
Gujarat Technological University, Gujarat, India

Abstract- Popularity of Wireless Sensor Networks (WSNs) is increasing continuously in different fields, as they provide efficient method of collecting valuable data from the surroundings for use in different applications. Routing in WSNs is the vital functionality that allows the flow of information generated by sensor nodes to the base station, while considering the severe energy constraint and the limitations of computational and storage resources. Indeed, this functionality may be vulnerable and must be in itself secured, since conventional routing protocols in WSNs provide efficient routing techniques with low power consumption, but they do not take into account the possible attacks. As sensor nodes may be easily captured and compromised, the classical cryptographic solutions become insufficient to provide optimal routing security, especially, for cluster-based WSNs, where cluster heads can be still among the compromised nodes. In this paper, we have proposed a light-weight IDS to detect black hole attack for OEERP protocol.

***Index Terms-* Wireless sensor network, Hierarchical WSN, cluster based routing protocol, security, Intrusion detection system, OEERP, SOEERP.**

I. INTRODUCTION

Wireless Sensor Network (WSN) consists of a collection of nodes that are able to sensing, computation and wireless communication. They offer an excellent opportunity to monitor/sense the physical or environmental conditions such as temperature, sound, pressure etc. As WSN Provide a bridge between the real physical and virtual worlds, so used in applications such as battlefield surveillance in military, industrial process monitoring and control, food processing, machine health monitoring and many more[1].

WSN is built of nodes from a few to several thousand or hundreds, where each node is connected to at least one sensor. Constraints like size and cost on sensor nodes results in constrains on energy, memory, computational speed and bandwidth. Each node in WSN has a radio transceiver with an intended antenna or collection to an external antenna, battery and a microcontroller-an electronic circuit for computation. Constraints like size and cost on sensor nodes results in constrains on energy, memory, computational speed and bandwidth [12].

Usually sensors are small in size and inexpensive. The nodes in WSNs are battery operated sensing devices with limited power supply and replacing or refilling the batteries is usually not an option. So, energy efficiency is one of the most important issues and designing power efficient protocols is critical for prolonging the lifetime.

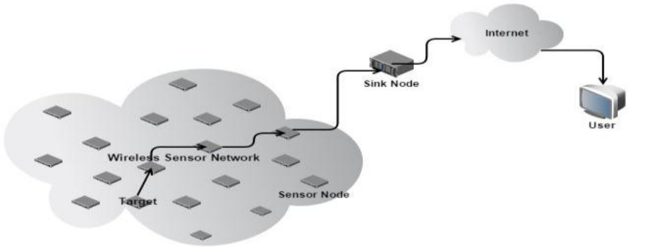

Figure 1 An example of WSN

Normally, sensor nodes are scattered in the sensing field, in the area where we want to monitor some environmental conditions. The data collected by sensor nodes is routed to the Base Station either directly or through other sensor nodes. The Base Station is either a fixed node or mobile node, which connects the sensor network to an infrastructure networks or to the Internet where users can access data and process it achieve some result as shown in Figure 1.

II. ROUTING IN WSN

The main task of sensor node is to sense data and sends it to the base station in multi hope environment for this routing is very essential. For computing routing path from sensor node to Base station (BS), there are number of routing protocols exist. Routing protocols are categorized mainly into 1) Based on Network structure and 2) based on Protocol Operation[9].

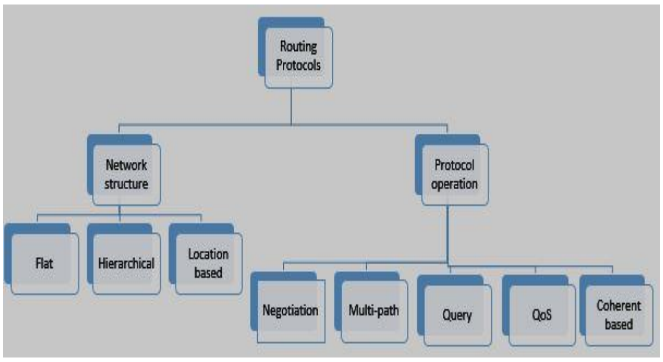

Figure 2 Routing in WSN

All the routing protocols are very useful for computing routing path, which highly affect the WSNs performance. So, development of the routing protocol should be concentrating on balancing the load among all the sensor nodes and prolonging the network lifetime[9].LEACH ,PEGASIS,OEERP etc. are examples of Hierarchical protocols.

III. ROUTING SECURITY IN WSN

Main security threats in WSN are: 1) Radio links are insecure and eavesdropping / injecting faulty information is possible in network. 2) Sensor nodes are not temper resistant .If it is compromised the attacker obtains all security information. Protecting confidentiality, integrity, and availability of the communications and computations is their motto keeping in mind that energy is very limited resource.

3.1 Routing attacks [1]

Due to lack of human monitoring of the network, it is possible to easily compromised sensor network. The attacks can be classified as active, passive, external and internal.

Active: The attacker exploits the weak link in the security protocol to launch attacks like packet modification, replaying etc.

Passive: The attacker obtains access to information without being detected. It is a kind of attack which is difficult to detect.

External: The attacker is external entity and has no rights to access the network.

Internal: The attacker gets authorization to access the network and deploys malicious node to compromise the sensor nodes and takes control of the network.

3.2 Why routing security of WSN differs from other networks? [13]

Routing in WSNs is more challenging due to the specific characteristics that distinguish WSNs from other wireless networks like cellular networks or ad hoc networks. Many new protocols have been proposed, taking into limitations and requirements of WSNs along with the application and architecture. Following are some important differences between them because of why routing security is different in WSN [13].

1)In ad hoc networks, every node is usually managed and handled by a human user. However, in a sensor network, every node is working totally independent by sending data and receiving control packets from a central system Base station (BS), which is managed by a human user.

2)Batteries and computing resources are more constrained in sensor nodes than in ad hoc nodes.

3)The purpose of sensor networks is very specific: measure the physical information (such as temperature, sound, ...) of its surroundings. Resulting, both hardware modules and communication/configuration protocols to be highly specialized.

4)Node density in sensor networks is higher than in ad hoc networks. But, sensor nodes have more chances to fail and disappear from the network, due to the battery constraints and the low physical security.

3.3 Problem Statement

The existing secure routing protocol in WSNs focused on presenting security system with key management schemes and cryptographic solutions. These protocols are very efficient to defense the external attacks but somehow they don’t treat the insider attacks as a serious issue. It is a major drawback for these protocols that they are not capable to detect compromised node in the network.

Since an insider attacker disposes, it can have hold of the relevant cryptographic keys and any possible security material to be part of the routing path. Thus, a compromised node may success to be a CH and it can perform several attacks on an entire group of sensor nodes. Moreover, cryptographic and key management solutions which able resist the outsider attackers and reduce the impact of the insiders couldn’t provide the desired security for routing in hierarchical WSNs, even if the network is having only a few malicious nodes. Thus various IDS are introduced to detect insider attacks which provide second line of defense.

3.4 IDS in WSN

In order to respond to the need to intrusion prevention in WSNs, many researchers have proposed several solutions.

In [10], energy efficient hybrid IDS (eHIDS) is introduced. This detection scheme combines both misuse and anomaly detection rules in order to identify abnormal data transfer in hierarchical WSNs. eHIDS agents are implanted only on clusters heads, which reduces energy consumption significantly. The anomaly detection model includes general attacks on integrity, delay and transmission range. Whenever an intrusion is detected, decision making module will generate an alarm. Authors claim that the proposed IDS has high detection rate, while it hasn't been evaluated with specific and various attacks.

In [11], a light weight ranger intrusion detection system is generated to link between ontology concept and intrusion detection system. . It is characterized by a particular architecture; the network should have one primary cluster head (PCH), ranger nodes (RN), member nodes(MN). This RIDS (Ranger Intrusion Detection System) mainly focuses on to detect Sybil attacks. Here, PCH is responsible for connectivity between WSN and base station communications. They also control ranger nodes. Ranger nodes collect information regarding respective member sensor nodes either periodically or non-periodically as per requirement. These ranger nodes sends isolation table to PCH time to time. Member nodes, who responsible for sensing the whole environment also translates information to ranger nodes after integration. If any exception of PCH is occurred, MN will raise alarm the amounts of MNs reaching threshold value.

In [3], a novel anomaly detection based security scheme for large scale sensor networks that exploits their stability in their neighborhood information. If each node can built a profile of its neighbor's behavior, these profiles would help to detect changes in them by monitoring received packet power levels and arrival rates. Here, the complexity of a detection algorithm depends on the number and characteristics of system features.

In [7], a hierarchical energy efficient intrusion detection system for detecting black hole attack is proposed. In this paper the proposed approach is based on control packets exchange between sensor node and base station. Each control packet contains the node identifier id, number of packets Nb sent to cluster head. Base station will compare this Nb of each node with the amount of packets received from its CH. In case of attack, BS will broadcast an alarm to all network nodes. The alarm packet contains id of detected CH. This proposed system is energy efficient as well as helps in detecting selective forwarding attack.

In [13], a novel technique to optimally watch over the communications of the neighbor sensor nodes is proposed on certain scenario. They have proposed a new technique called spontaneous watchdog, where some nodes are able to choose independently to monitor the communications in their neighborhood. For the sake of performance detection entities called agents are divided in to two types global and local. Local agents are responsible to monitor local activities and the information sent and received by the sensor. Global agents should watch over communications and behaves as a watchdog. This technique relies on the broadcast nature of sensor communication. Here anomaly detection technique can be used for monitoring certain parameters and limits.

IV. THE PROPOSED METHODOLOGY: SECURE AND OPTIMIZED ENERGY EFFICIENT ROUTING PROTOCOL (SOEERP)

In order to address the problem of insider attackers for routing security in Hierarchical WSN, we propose a protocol that detects black hole attacks as well it is energy efficient called SOEERP. Black hole attack is the most dangerous attack, especially when applied by CHs attackers, because of their enormous impact on network performance.

The integration of our IDS, in secure hierarchical protocols, takes place just after data dissemination Phase within clusters, and just before a new phase of topology reconstruction.

For energy efficiency unlike the most existent IDSs which have high energy consumptive alerting systems, where alarm messages are directly sent to the BS each time an intrusion is detected. Whereas our IDS present a lightweight alerting system, consists of two types of alerting messages: local and general alerts.

Local alerts: They have a little energy cost, and are generated frequently to alert the nodes in its range about compromised CH.

General alerts: They are raised periodically, depending on threshold reaching. This leads to the simplicity and low energy consumption.

4.1 Network architecture

- Our proposed IDS is designed for cluster based WSNs, especially those where clusters are dynamically and periodically formed. Following are some key points which we have to take in consideration.

- Each cluster should have a few of Control & Monitor nods(CMs) that control the behavior of their CH.
- CMs are selected such in number that they are able to cover the whole cluster range and also able to work efficiently. The goal of proposing this IDS is to determined according to a tradeoff between detection effectiveness and energy saving. Choosing a few numbers of MNs affects the detection accuracy, where a large number introduces network overhead and energy exhaustion.
- CMs are selected dynamically and in random manner, to avoid predictability.
- A CM just performs monitoring, data sensing and communication functionalities not the detection task.
- Each time clusters change, the selected CMs change as well.

4.2 Proposed System model

Here, it is required that each sensor node including CM nodes has a local list called the intruder list. When member sensor nodes send their data messages to the CH, CM who is monitoring the CH by listening exchanged messages during that time slot would check whether CH is sending those messages to BS or not. If the CM finds that there is no data message is sent by CH, it would consider that CH an attacker and identified this attack as black hole attack.

Now, CM would put CH's identifier in its intruder list and creates a local message containing that CH's id to all the neighboring nodes that are in the range. If the length of intruder list reaches up to threshold value which is priori CM would create a general alarm and sent it to BS. This is shown to the Figure 8.

The threshold value should be carefully defined; a reduced value leads to overload the network and a big value affects the process of isolating the malicious node coordination with the BS. On each time it receives such a general alert message, the BS updates its proper intruder list by adding the new intruders, allowing it to revoke the susceptible incoming malicious messages.

On receiving that local alert message, sensor nodes update their intruder lists by adding malicious node ID. The monitoring and detection algorithm would make sure that detected attackers, whose IDs appear in nodes blacklist, will never be chosen as CHs in the future clusters reconstructions. This allows then black hole prevention.

Insider malicious nodes finding themselves isolated from being CHs may transmit falsified reports to the BS. So, for a complete isolation, CMs as well as the legal sensor nodes should send general alarms carrying their intruder lists to the BS as shown in the figure 8. As direct communication with BS costs a lot of energy, general alerts are sent only if the number of intruders are goes beyond or equal to the pre-defined threshold.

In order to validate our assumption, we have chosen the protocol OEERP to be equipped with our proposed intrusion detection system. SOEERP operation s, therefore, divided into the following phases:

- Cluster formation, isolation of previously detected attackers and CMs selection.
- Information processing phase
- Data dissemination phase.
- Intrusion detection and alerting phase.

The above proposed IDS would start monitoring in data dissemination stage and doing all the blocking or isolating malicious nodes and alerting other nodes in intrusion detection and alerting phase.

In a new time slot- next time slot, when clusters would reconstruct that time every sensor nodes would check the received Advertisement message broadcasted by probable CH and compare identifier of that candidate to its intruder list. And if it is not there, it would send approval message Join to that candidate.

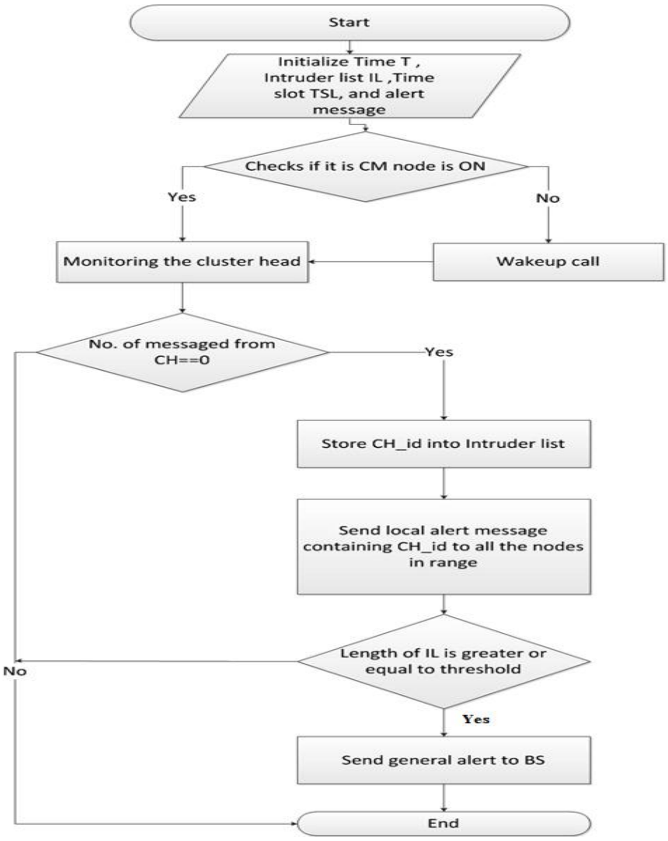
Start
Initialize Time T , Intruder list IL ,Time slot TSL, and alert message
Checks if it is CM node is ON
Yes
No
Monitoring the cluster head
Wakeup call
No. of messaged from CH==0
Yes
Store CH_id into Intruder list
Send local alert message containing CH_id to all the nodes in range
No
Length of IL is greater or equal to threshold
Yes
Send general alert to BS
End

Figure 3 Work flow of IDS deployed on CM node

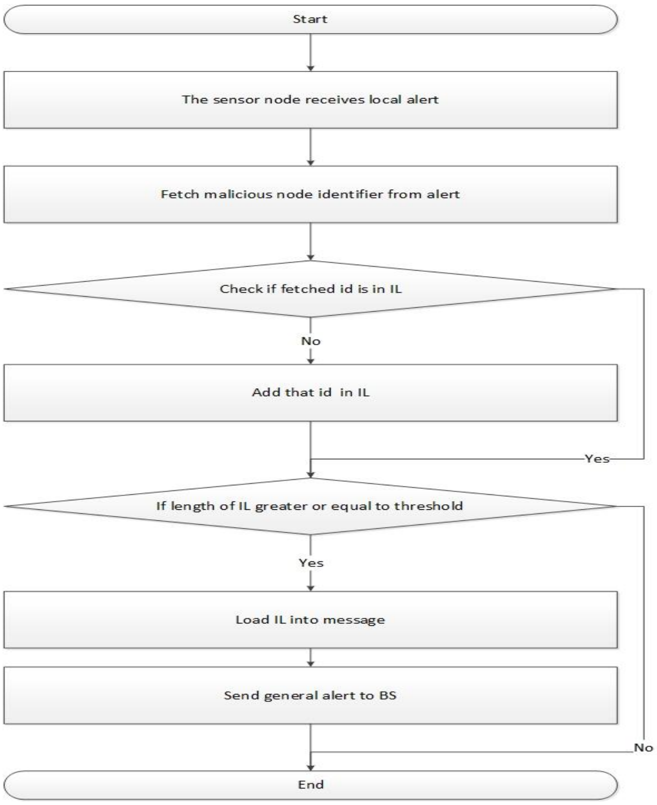
Start
The sensor node receives local alert
Fetch malicious node identifier from alert
Check if fetched id is in IL
No
Add that id in IL
Yes
If length of IL greater or equal to threshold
Yes
Load IL into message
Send general alert to BS
No
End

Figure 4 detecting code deployed on sensor nodes

V. EVALUATION AND SIMULATION RESULT

Physically implementation of routing strategy is not possible in WSN due to cost factor, so various routing simulator used for performance measurement. Simulation of the proposed protocol requires various different features which are available in different simulator tools. The selection of the simulator for proposed protocol may vary based on the requirements.

In order to evaluate performances of SOEERP protocol, we have used the network simulator NS2. We have implemented SOEERP protocol on the MIT's LEACH patch for ns2 [14]. The assumed network model is composed of 100 sensor nodes, randomly deployed on a surface of 100m*100 m, where all nodes are supposed fixed. Simulation Time would be 30 sec to 100 sec and packet length would be 512 bytes. The number of clusters would be 5 with each cluster has one CM node.

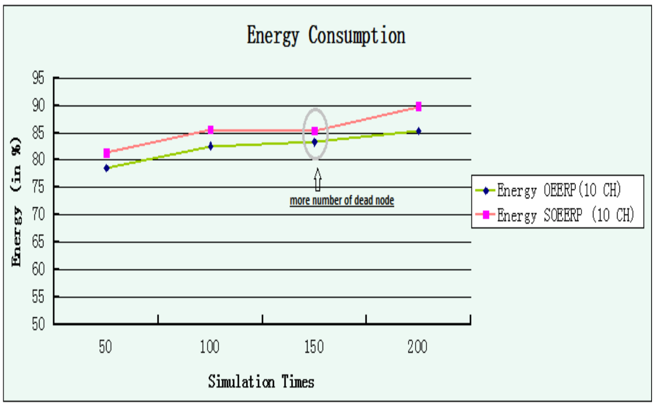

Figure 5 Energy consumption evaluation

Fig 3 shows the energy consumption scenario for OEERP and SOEERP. As proposed system-SOEERP is an IDS deployed on OEERP ,it consumes a little more energy compare to the OEERP.

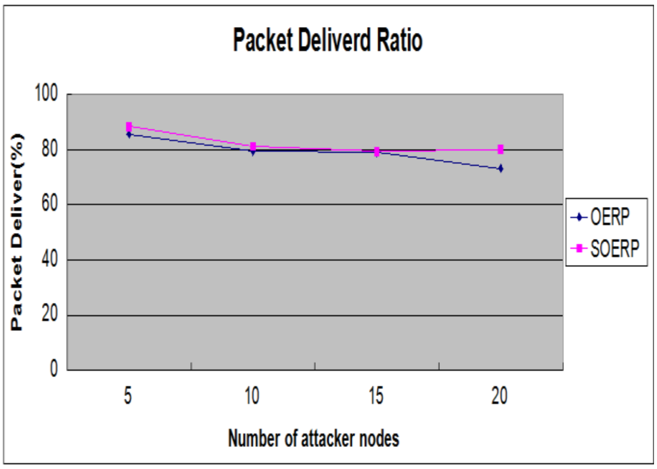

Figure 6 Packet delivery Ratio

The results for packet delivery ratio shown in Fig 4 shows that proposed SOEERP has good packet delivery ratio compare to OEERP. As SOEERP is able to detect malicious CH and is successfully avoiding malicious node to choose as CH, packet delivery ratio increases.

VI. CONCLUSION & FUTURE WORK

Black hole is one of the most malicious attacks that targets sensors routing protocols. we conclude that hierarchical routing protocols integrate intrusion detection mechanisms, so that malicious behaviours may be detected, and the responsible nodes This type of attacks can have devastating impact on hierarchical routing protocols. Several secure solutions have been proposed to secure WSNs from black hole attacks. However, most of these solutions are complex and energy inefficient. For this reason, could be isolated. Our scheme involves setting up light-weight IDS, called SOEERP that is energy efficient as well. From our evaluation, it can be implied that the solution works better in black hole attack. It increases packet delivery ratio as well as throughput in comparison and consumes only little amount of energy more than older protocol.

We are looking forward to evaluate results for using this proposed IDS on other hierarchical protocols and enhance their routing security.

REFERENCES

[1] Abror Abduvaliyev, Al-Sakib Khan Pathan, Jianying Zhou, Rodrigo Roman, and Wai- Choong Wong, “On the Vital Areas of Intrusion Detection Systems in Wireless Sensor Networks”, IEEE Communications Surveys & Tutorials, Vol. 15, No. 3, Third Quarter 2013,pp. 1223 – 1237

[2] Bo Sun And Lawrence Osborne,Yang Xiao And Sghaier Guizani, “Intrusion Detection Techniques In Mobile Ad Hoc And Wireless Sensor Networks”, IEEE Wireless Communications October 2007,pp. 56 – 63

[3] Onat and A. Miri, “An Intrusion Detection System for Wireless Sensor Networks, Wireless and Mobile Computing”, Networking and Communications, vol. 3, 2005, pp. 253-259

[4] W.R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, “Energy-efficient communication protocol for wireless micro sensor networks”, System Sciences, 2000. Proceedings of the 33rd Annual Hawaii International Conference, IEEE

[5] S. Lindsey, and C. Raghavendra, “PEGASIS: Power-Efficient Gathering in Sensor Information Systems”, Aerospace Conference Proceedings, 2002. IEEE , vol. 3, pp.1125 - 1130

[6] K. Kishan Chand, P Vijaya Bharati and B. Seetha Ramanjaneyulu, “Optimized Energy Efficient Routing Protocol for Life-Time Improvement in Wireless Sensor Networks”, IEEE-International Conference On Advances In Engineering, Science And Management (ICAESM -2012) March 30-31, 2012,pp. 345 – 349

[7] Samir Athmani, Djallel Eddine Boubiche and Azeddine Bilami, “Hierarchical Energy Efficient Intrusion Detection System for Black Hole Attacks in WSNs”, Computer and Information Technology (WCCIT), 2013 World Congress on Date 22-24 June 2013,pp. 1 – 5

[8] Jamal N. Al-karaki and Ahmed E. Kamal, “Routing Techniques in Wireless Sensor Networks: A Survey”, IEEE Wireless Communications , December 2004, vol. 11,Issue:6

[9] Suraj Sharma and Sanjay Kumar Jena, “A Survey on Secure Hierarchical Routing Protocols in Wireless Sensor Networks”, *ICCCS’11* February 12-14, 2011, Rourkela, Odisha, India, pp. 146-151

[10] Abror Abduvaliyev, Sungyoung Lee and Young-Koo Lee, “Energy Efficient Hybrid Intrusion Detection System for Wireless Sensor Networks”, 2010 International Conference on Electronics and Information Engineering (ICEIE 2010), 1-3 Aug. 2010 vol. 2,pp. 25-29

[11] Chia-Fen Hsieh, Yung-Fa Huang and Rung-Ching Chen, “ A Light-weight Ranger Intrusion Detection System on Wireless Sensor Networks”, 2011 Fifth International Conference on Genetic and Evolutionary Computing, pp.49–52

[12] Ismail Butun, Salvatore D. Morgera and Ravi Sankar, “A servey of Intrusion Detection Systems in Wireless Sensor Networks”, IEEE Communications and Surveys & Tutorials, vol. 16,Issue-1, First quarter 2014,pp. 266-282

[13] Rodrigo Roman, Jianying Zhou and Javier Lopez, “Applying Intrusion Detection Systems to Wireless Sensor

Networks", in Consumer Communications and Networking Conference, 2006, pp. 640-644

[14] NS2 documentation and Updates available: http://www.isi.edu/nsnam/