Comparative Analysis of Secure Routing in WSN

Ouafaa Ibrihich, Salah-ddine Krit, Jalal Laissiri and Said El Hajji

Abstract— **Wireless sensor networks are becoming significantly vital to many applications, and they were initially used by the military for surveillance purposes. One of the biggest concerns of WSNs is that they are defenseless to security threats. Due to the fact that these networks are susceptible to hackers; it is possible for one to enter and render a network. However, WSN presents many challenges. These networks are prone to malicious users attack, because any device within the frequency range can get access to the WSN. There is a need for security mechanisms aware of the sensor challenges (low energy, computational resources, memory, etc.). Thus, this work aims to simulate a secure routing protocol for WSN by using trusted frame works called SAODV (Secure Ad hoc On-Demand Distance Vector). The Trust Scheme evaluates the behavior of all nodes by establishing a trust value for each node in the network that represents the trustworthiness of each one thereby identifies and eliminates the malicious nodes. It also observes node's mobility, number of neighbors each node has, number of packets generated and forwarded by the neighboring nodes, and the past activity of the node.**

Index Terms— **Security, Attacks, Wireless Sensor Networks (WSN), Routing protocols, SAODV.**

I. INTRODUCTION

A Wireless sensor network is a collection of nodes organized into a cooperative network [1]. Each node consists of processing capability (one or more microcontrollers, CPUs or DSP chips), may contain multiple types of memory (program, data and flash memories), have a RF transceiver (usually with a single Omni-directional antenna), have a power source (e.g., batteries and solar cells), and accommodate various sensors and actuators. The nodes communicate wirelessly and often self-organize after being deployed in WSN fashion. Wireless networks are gaining popularity to its peak today, as the users want connectivity in terms of wireless medium irrespective of their geographic position. There is an increasing threat and various attacks on the Wireless Network.

However, each node in the network has the ability to discover its neighbors and to construct routes to reach other nodes in the collection. Like other networks, sensor networks are vulnerable to malicious attack; however, the hardware simplicity of these devices makes defense mechanisms designed for traditional networks infeasible. This work explores the Denial-of-Service (DoS) attack, in which a sensor node is targeted [2].

II. Wireless Sensor Network: An Overview

The characteristics of WSNs are discussed from two perspectives: from the nodes that make up the network, and from the network itself.

The very idea of a wireless network introduces multiple venues for attack and penetration that are either much more difficult or completely impossible to execute with a standard, wired network. This inherent limitation makes WSNs especially sensitive to several key types of attacks. In contrast to resource-rich networks such as the Internet, a WSN is less stable, more resource-limited, subject to open wireless communication, and prone to the physical risks of in-situ deployment. These factors increase the susceptibility of WSNs to distinct types of attacks.

Attacks can be performed in a variety of ways, most notably as denial of service attacks, but also through traffic analysis, privacy violation, node takeover, attacks on the routing protocols, and attacks on a node’s physical security which all are out of the scope of this research. In this paper, we first address some common denial of service attacks and then describe the most famous defensive strategies against them.

Security in WSNs can be defined as the method of protecting a prospective application against all known types of attack. Attacks including denial-of-service (DOS), traffic analysis, multiple identity/node replication, confidentiality and physical tampering are all areas for concern within WSN security architecture design, it is extremely important to ensure that all known attacks are defended against when designing a security system for a WSN. The success of the application will depend largely upon its reliability and robustness against attack [3].

III. ATTACKS IN WIRELESS NETWORKS

Wireless networks are more susceptible to attacks because of their shared physical medium, open transmission of radio frequencies [4].

A. Vulnerabilities of Wireless Sensor Networks

A typical wireless sensor network is expected to give a certain data that the user is actively enquiring about after some amount of time. Many attack schemes tend to stop the proper performance of sensor networks to delay or even prevent the delivery of data requested by user. Despite the

O. Ibrihich is currently an administrator of informatics with Polydisciplinary Faculty of Ouarzazate, Ibn Zohr University, Agadir, Morroco. (e-mail: wafaa.ibrihich@gmail.com).

S. Krit is currently a professor of informatics with Polydisciplinary Faculty of Ouarzazate, Ibn Zohr University, Agadir, Morocco. (e-mail: krit_salah@yahoo.fr).

J. Laassiri is a professor at Faculty of Sciences of Kenitra, Department of Computer Sciences, Ibn Tofail University, Morocco. (e-mail: laassiri.jalal@gmail.com).

S. El Hajji, Professor of Higher Education at Mohammed V - Agdal University, chief of Laboratory MIA, Faculty of Sciences, Rabat, Morocco. http://www.fsr.ac.ma/mia/elhajji.htm. (e-mail: elhajji.said@gmail.com).

fact that the term attack usually refers to an adversary's attempt to disrupt, undermine, or destroy a network, a Denial-of-Service (DoS) attack refers to any event that diminishes or eliminates a network's ability to perform its expected function. Such a technique may be helpful in specific applications such as utilizing the best of these attacks to find the weak tips of presented protocols at different layers. These attacks consequently would expose weaknesses that lead to effective countermeasures.

B. Denial of Service Attack in Wireless Sensor Networks

The aim of DoS attack is to make services unavailable to legitimate users, and current network architectures allow easy-to-launch and hard-to-stop DoS attacks. Particularly challenging are the service-level DoS attacks, whereby the victim links are destroyed and flooded with legitimate-like requests attack, in which wireless communication is blocked by malicious radio interference. These attacks are overwhelming even for massively resourced services, and effective and efficient defenses are highly needed.

Denial of Service (DoS) is a common type of cyber-attack over the Internet. The purpose of DoS is to make a computer's resources unavailable to its intended users. One way to launch a DoS attack is by sending malformed traffic to the target or by sending a huge amount of normal traffic which will overload the target's buffer. To be more effective, attackers often use many compromised machines, rather than just one, as a source for the attack. There are many security attacks which are considered under in Dos [5].

C. Problematic

Denial-of-Service attack in wireless sensor network occurs due to intentional intrusion attack or unexpected node failure [6], [7].Various software bugs, unexpected sensor node failure, exhausted power supply system, environmental disaster, complication in data transmission and communication or even intentional intruder attack may execute DoS attack. Often the outsiders try to weaken or destroy a network or cause an interruption in secure data communication by sending loads of unnecessary data packets to the victim nodes and therefore exhibit DoS attack [8].

Attacker's Distribution

Clearly, if only one node on the border of the network is attacked, the impact on performance metrics that determine the "health" of the network will be minimal. On the other hand, if the attacked node is a one through which many routes must pass, the impact of the attack will be more noticeable; assuming that attackers are poorly informed, though it is fair to expect that they wouldn't be able to distinguish a border node from an internal node. For this reason, we assume that every node in the network is equally likely to be attacked. In our model, we divide the whole network into k certain attack zones where k represents the previously estimated number of attackers. Each such zone shows the zone of attack or the territory of the attack node. Zone size is -controlled by the number of nodes in the network which defines a minimum bound on the number of serving attackers to cause the desired effect in degrading network performance characterized by decreasing the throughput at the sink and increasing the corresponding delay of the delivered data [9].

Fig 1: below demonstrates the division of the network in to k attack zones where k equals the number of attackers represented by red circles, are legitimate sensors, represented by circles in black.

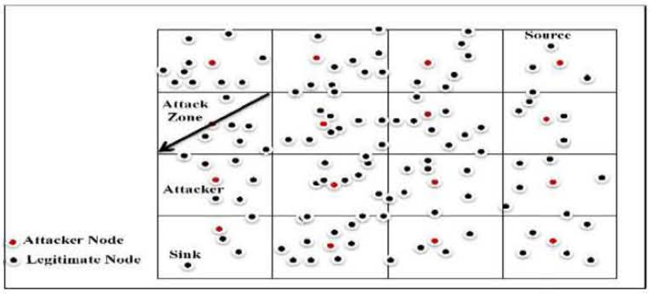

Fig 1: Attacker distribution into attack cells throughout the network

IV. SIMULATION SETUP

A. Simulation Tools

The NS-2 simulator is a discrete event-driven network simulator, which is popular with the networking research community [10]. It was developed at the University of California at Berkeley and extended at Carnegie Mellon University, CMU, to simulate wireless networks [11]. These extensions provide a detailed model of the physical, link layer behavior of a wireless network, and allow arbitrary movement of nodes within the network. It includes numerous models of common Internet protocols including several newer protocols, such as reliable multicast and TCP selective acknowledgement. Additionally, different levels of configurations are present in NS-2 due to its open source nature, including the capability of creating custom applications and protocols as well as modifying several parameters at different layers.

The simulator is written in C++, accompanying an OTCL script language based on Tcl/Tk. The researcher defines the network components such as nodes, links, protocols and traffic using the OTCL script. NS-2 uses OTCL as the interface to the user (Fig 2). This script is then used with NS, the simulator, to conduct the desired simulation, and as a result outputs traces at different selective layers. The output data within the trace output files is then filtered and extracted using statistical analysis software like excel/access program. The extracted relevant data is then used to evaluate performance by manipulating various metrics such as delays, throughput, overheads etc.

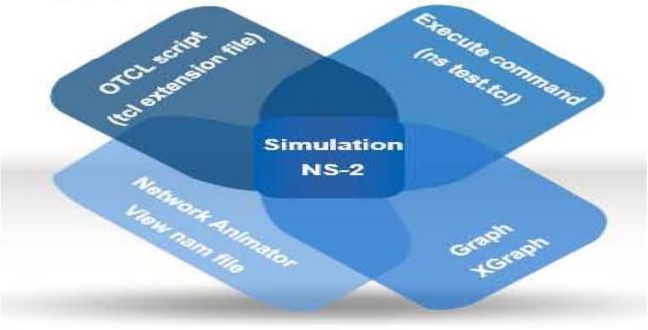

Fig 2: Simulation Overview

B. Simulation Environment

We simulated DoS attack in NS-2.35. We also use NAM visualization tool to show the Network animator.

The following are the configurations set as per the assumed simulation context:

Parameters	Value
Simulator	NS-2 (version 2.35)
Channel type	Channel/Wireless channel
Radio-propagation model	Propagation/TwoRayGround
Network interface type	Phy/WirelessPhy
MAC Type	Mac /802.11
Interface queue Type	Queue/DropTail\PriQueue
Link Layer Type	LL
Antenna model	Antenna/OmniAntenna
Maximum packet in ifq	20
Number of mobile node	50
Traffic type	TCP
Simulation Time	500 sec
Routing Protocols	AODV
Nominal bit rate	2 Mb/s
Node speed	1m/s – 15m/s
Transmission rate	4 packets/sec
Area of simulation	1000m * 300m

Table 1: Simulation parameters for scenario1

For describing the working of DoS attack three steps are discussed as Route Request (RREQ), Route Reply and Propagation of route reply (PREP):

In order, the malicious node M0 begins by broadcasting a RREQ (Route REQuest) message (malicious packets). Route request will be broadcasted in the manner of multi node hops. In Fig 3 during path discovery process, sender broadcasts RREQ to its neighbouring nodes i.e. 1, 5, 10, 15, and 20. The neighbouring nodes will forward RREQ further to their neighbours.

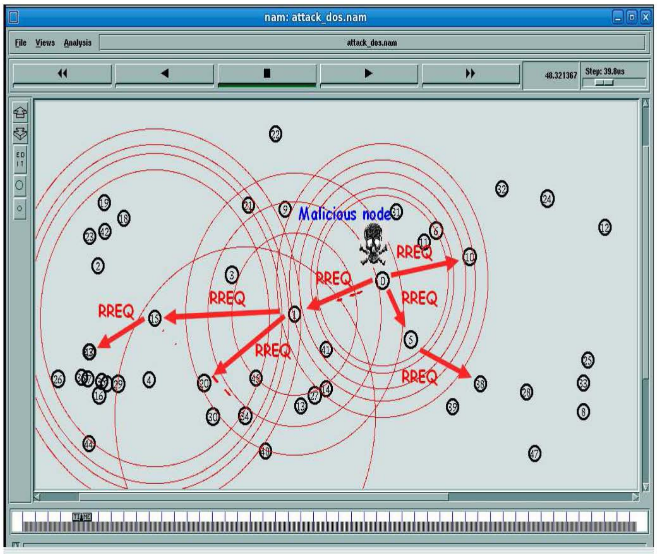

Fig 3: Malicious node sending Route REQuests to get access to different nodes

After getting the route request to destination from the sender, destination will unicast a route reply (RREP) packet to source node 0 (Fig 4).

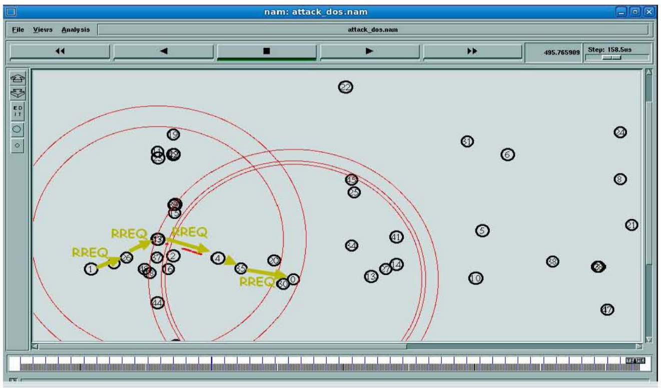

Fig 4: RREP message from destination to malicious node

Whenever node 0 detects a link break from link layer, the source and end nodes are notified by propagating an RERR packet similar (malicious packets) to different nodes (Fig.5).

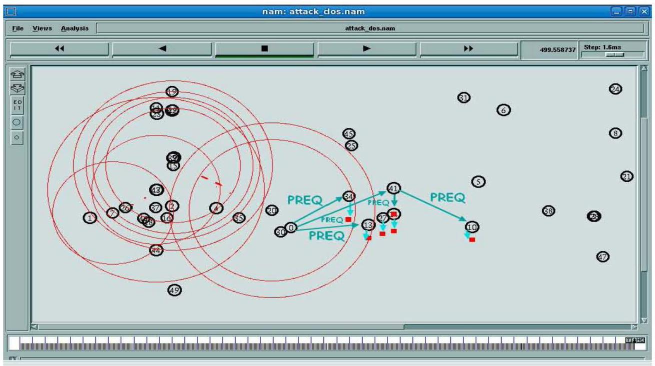

Fig 5: PREQ message from malicious node to destination

The attacker can allow his replica nodes to randomly move or he could move his replica nodes in different patterns in an attempt to frustrate proposed scheme. We also assume that the base station is a trusted entity. This is a reasonable assumption in mobile sensor networks, because the network operator collects all sensor data and can typically control the nodes operation through the base station. Thus, the basic mission of the sensor network is already completely undermined if the base station is compromised.

V. AODV AND SAODV ROUTING PROTOCOLS

A. Ad-Hoc on Demand Distance Vector Routing Protocol

AODV is a reactive routing protocol which creates a path to destination when required. Routes are not built until certain nodes send route discovery message as an intention to communicate or transmit data with each other [12]. This routing protocol uses two phases. In phase one route discovery is done. In phase two route maintenance is done. It uses three control messages namely:

Route Requests (RREQs)

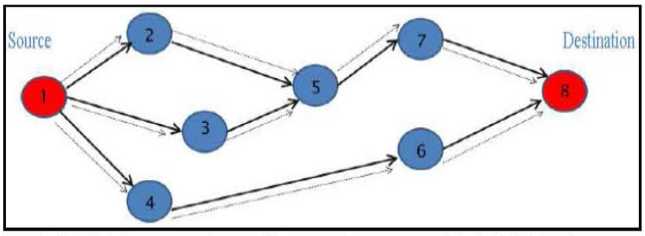

Fig 6: Propagation of Route Request (PREQ) Packet

Route Replies(RREPs)

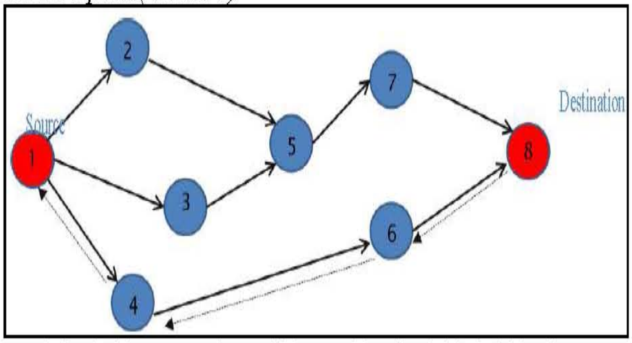

Fig 7: Propagation of Route Reply (PREP) Packet

Route Erros (RERRs)

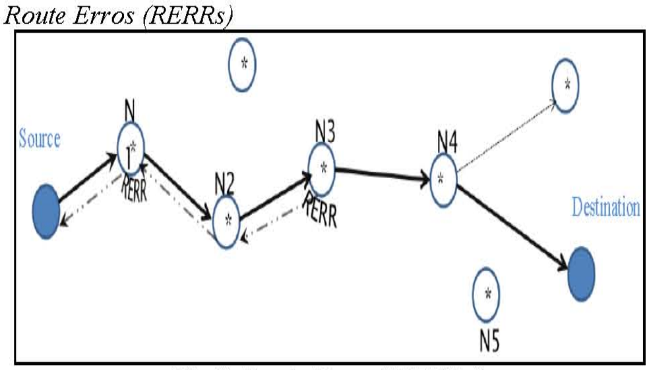

Fig 8: Route Errors(RERRs)

The RREQ and RREP messages are used in phase one whereas RRER control message is used in phase two. The steps to be followed in AODV protocols are as follows: [13]

i. Source node broadcasts RREQ message. It contains source and destination address, sequence number and broadcast id.

ii. If the next node is the destination then it replies with RREP message or else message is forwarded to next node.

iii. When forwarding the RREQ message node maintains broadcast id, source address and maintains a reverse route.

iv. Sequence number helps in route updation and helps in getting fresh enough route to the destination.

v. Destination node on receiving RREQ then sends a unicast RREP message to the source node on the same path that was created during RREQ.

B. Secure AODV Routing Protocol

SAODV is an extension to AODV. It uses asymmetric cryptography to secure AODV's routing messages. SAODV uses Digital Signatures to protect the non-mutable data in the RREQ and RREP messages. The four basic operations performed for the Route Establishment are 1.Route Discovery 2.Route Request 3.Route Reply and 4.Route Maintenance (Fig 9).

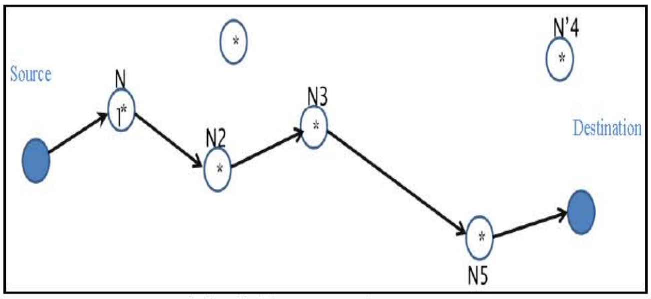

Fig 9: Route maintenance

Before entering the network, each node obtains a public key certificate from a trusted certificate server. There are End-to-end authentication between source and destination and Hop-to-hop authentication between intermediate nodes. Hash chains are used in SAODV to authenticate the hop count of the AODV routing. Source broadcasts signed RDM (Route Discovery Message) along with its own certificate. RDM contains the source IP address, along with a source-specific nonce (to detect duplicates) [14].

VI. Related Works

In this paper, first I want to show the comparison between the packet loss of AODV and SAODV. We have different number of nodes and simulation parameter by which we can do analysis. The graph shown the packet loss and packet received for AODV and SAODV. Further, we can change the simulation parameter and time and see the changes in graph.

We can have different parameter for better results. The table 2 shows the simulation parameters for our scenario:

Parameters	Value
Simulator	NS-2 (version 2.35)
Channel type	Channel/Wireless channel
Radio-propagation model	Propagation/TwoRayGround
Network interface type	Phy/WirelessPhy
MAC Type	Mac /802.11
Interface queue Type	Queue/DropTail\PriQueue
Link Layer Type	LL
Antenna model	Antenna/OmniAntenna
Maximum packet in ifq	30
Area for simulation	200 * 200
Number of mobile node	10
Traffic type	TCP
Simulation Time	50 sec
Routing Protocols	AODV, SAODV

Table 2: Simulation parameters for scenario2

After simulation, NS2 outputs a trace file, which can be interpreted by many tools, such as NAM and Xgraph. We create a simulation scenario using NS-2 Scenario Generator [15]. Table 2 shows the network parameter definition in the TCL file. The first parameter tells the simulator that nodes transmits and receives packets through wireless channels. We have used the IEEE 802.11 standard, which specifies the media access control and the physical layer [16].

The Fig 10 shows the X graph of comparison between AODV and SAODV. By the Figure, we see that as the simulation start the packet received and packet loss is initially zero, because initially there is no CBR connection and nodes taking their right place. As the CBR connections establish between the nodes the number of packet received increases but no packet loss is there, it means all generated packets are being received by the nodes. But the packet loss increases substantially on the simulation time increases (in AODV). Finally, the packet received is more than the packet loss and nodes taking their right place (in SAODV). As the CBR connections establish the number of packet lost increases very much as compare to packet received. It shows that the nodes are dropping mostly generated packets.

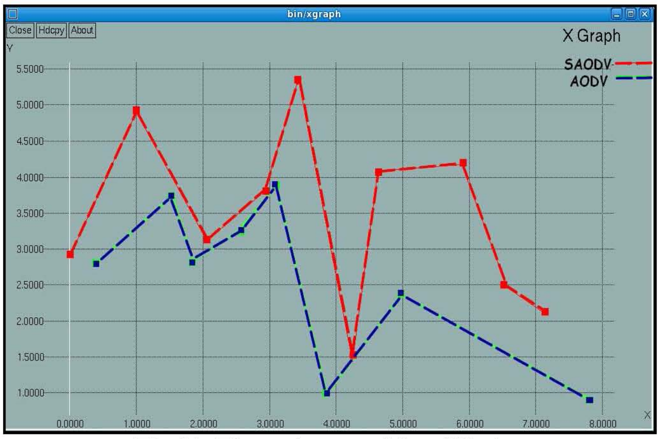

Fig 10: Throughput vs. No of Nodes

From the graph (Fig 11), it is clear that the throughput of dropping packets (coming from the malicious node) at the destination node is low using the AODV protocol. The throughput of dropping packets at the receiving node becomes high using the secure AODV. This means that using this secure routing protocol allow rejecting malicious packets. Then malicious node will not be able to send malicious packets on the WSN.

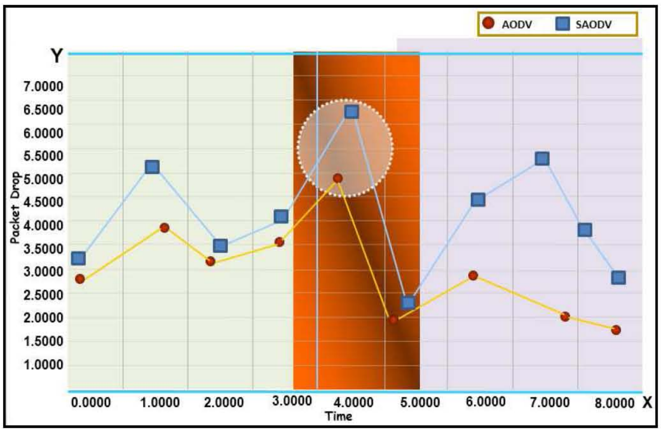

Fig 11: Throughput of dropping packets

Packet Delivery Fraction

The packet delivery ratio in this simulation is defined as the ratio between the number of packets sent by constant bit rate sources and the number of received packets by the CBR sink at destination.

From the graph (Fig 12), SAODV performs better than AODV in case of packet delivery fraction and goodput because the number of nodes is less and no periodic update is maintained in SAODV.

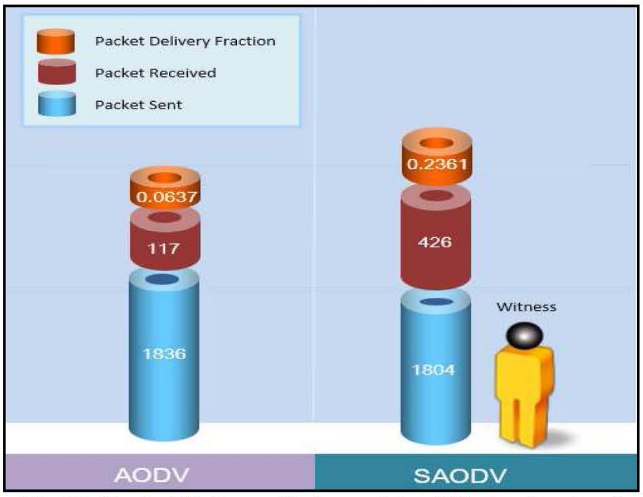

Fig 12: Packet Delivery Ratio vs. No of Nodes (sent and received)

VII. Conclusion and Future Works

Secure routing is vital to the acceptance and use of sensor networks for many applications, but we have simulated that currently routing protocols for these networks are insecure. In this paper, we have used an approach based on changing the packet transmission frequency in the AODV protocol, which is a reactive protocol. The goal is to avoid the DoS attack. We have shown an attack scenario, which we have simulated using NS-2.

For future work, we intend to simulate security protocols for aggregation and localization algorithms in WSN's, then add a switching technique from one protocol to another, based on sensor states (energy, mobility, connectivity, vicinity, etc.). At the end, we will have a secure and context aware protocol.

References

[1] Ilyas M, the Handbook of Ad-Hoc Wireless Networks. 2008 CRC Press, Florida.

[2] Huda Bader Hubboub, "Denial of Service Attack in Wireless Sensors Networks", 2010.

[3] David Boyle and Thomas Newe, "Securing Wireless Sensor Networks: Security Architectures", VOL. 3, NO. 1, JANUARY 2008.

[4] Shalini Jain and Dr.Satbir Jain," Detection and Prevention of Wormhole attack in mobile Ad hoc networks", International Journal of Computer Theory and Engineering, Vol. 2, No. 1, pp.78-86, February, 2010.

[5] G. C. Kessler, "Defences Against Distributed Denial of Service Attacks", November 2000, http://www.garykessler.net/library/ddos.html, Retrieved 10/30/2008.

[6] Wood, A. D. and Stankovic, J. A., "Denial of Service in Sensor Networks", Computer, October 2002, Vol. 35, Issue 10, pp. 54 - 62.

[7] Blackert, W.J., Gregg, D.M., Castner, A.K., Kyle, E.M., Hom, R.L., and Jokerst, R.M., "Analyzing interaction between distributed denial of service attacks and mitigation technologies", Proc. DARPA Information Survivability Conference and Exposition, April 2003, Vol. 1, pp. 26 – 36.

[8] Tasneem Halim and Md. Rafiqul Islam, "A Study on the Security Issues in WSN", Volume 53– No.1, September 2012.

[9] Huda Bader Hubboub, "Denial of Service Attack in Wireless Sensors Networks", 2010.

[10] K. Fall and K. Varadhan, "Editors ns Notes and Documentation," The VINT Project, UC Berkeley, LBL, USC/ISI, and Xerox PARC, Nov. 1997. Available: http://wwwmash. cs.berkeley.edu/ns

[11] P Pancardo, JC Dueñas, "A proposal for System Architecture to Integrate Scarce resources Wireless Sensors Neworks into Ubiquitous Environments". [Online], Available: http://ftp.informatik.rwth-aachen.de/Publications/CEUR-WS/Vol-208/paper23.pdf