International Journal of Soft Computing and Engineering (IJSCE)
ISSN: 2231-2307, Volume-1, Issue-1, March 2011

Evaluation of Security Conditions of Protocols for Data Routing in Wireless Sensors Networks

Tejpal Singh, Vinod Kumar, Khushboo Saxena, Akanksha Saxena

***Abstract*— A wireless sensor networks have recently emerged as successful technologies in a number of application domains. WSN design is influenced by many factors such as transmission errors, network topology and power consumption. Security in wireless sensor network is a challenging task; the need to build security services into them remains however a considerable challenge as the hardware used often shows serious processing and energy limitations. This work evaluates the impact of a security conditions and robustness criteria of routing protocols for WSN. Some of ITS features are not found in existing WSN simulation systems. It will provide the opportunity to implement and evaluate routing algorithms are designed to be that secure but for which there are in the experimental studies on the robustness and real impact of designed security mechanisms. This evaluation will focus primarily on examining the effectiveness of the provided security mechanisms. Additionally, it will also assess the impact of these mechanisms in relation to energy consumption, reliability, latency and resistance of the protocol, regarding the coverage and the scale of the network.**

Index Terms— security system, wireless sensor network, routing algorithms, attacks

I. INTRODUCTION

Sensors integrated into structures, machinery, and the environment, coupled with the efficient delivery of sensed information, could provide tremendous benefits to society. Potential benefits include: fewer catastrophic failures, conservation of natural resources, improved manufacturing productivity, improved emergency response, and enhanced homeland security.[16]

Long wire bundles represent a significant installation and long term maintenance cost, limiting the number of sensors that may be deployed, and therefore reducing the overall quality of the data reported. Wireless sensing networks can eliminate these costs, easing installation and eliminating connectors. WSN have characteristics of self-organization, and can be formed by a smaller or larger number of sensors, enabling small to cover large areas of monitoring. An environment of installing a network can be a building, an industrial plant, a combat area, a wide area monitoring of a natural habitat, a vehicle or the human body.

Manuscript received March 7, 2011..

Tejpal Singh ME Student of Delhi College of Engg. Main road Bawan Delhi (110042) INDIA(tejpal1985@gmail.com)

Mr. Vinod Kumar Assistant Professor in Delhi College of Engg. Main road Bawan Delhi (110042) INDIA(, k_vinod70@hotmail)

Ms Khushboo Sexsena Assistant Professor in *Techn ocrats Institute Of Technology Bhopa(M.P).India(*kskhushboosaxena[19]6@gmail.com*)*

Ms Akanksha Saxena Assistant Professor in *Suresh Gyan Vihar University Jaipur (Rajsthan) India(*akanksha.saxena23@gmail.com*)*

A wireless sensor network (WSN) generally consists of a base station (or "gateway") that can communicate with a number of wireless sensors via a radio link. Data is collected at the wireless sensor node, compressed, and transmitted to the gateway directly or, if required, uses other wireless sensor nodes to forward data to the gateway. The transmitted data is then presented to the system by the gateway connection.

Wireless sensor technologies enable two primary functions. The first is monitoring, for which information flows from the field to the user. The second is control, that is, management of the sensor system itself or the environment in which it is embedded. Such distributed monitoring and control within a local region, based on the sensors and the nodes into which they are incorporated, are qualitatively new capabilities. Because wireless sensor systems can be integrated with the cellular-, satellite-, and Internet-communication systems and networks, information both from the monitoring function and for control can span the globe, even if the wireless sensor technology is local in its reach. The more specific functions that wireless sensor technologies will perform are distributed and collaborative sensing, detection, and tracking; location determination and event recording; computing and signal processing; data and information management, aggregation and storage; and query processing. Their behavior will be collaborative, and it may also evolve in response to the conditions they encounter.

Dozens of applications for wireless sensor networks have been described. The applications can be grouped into several major areas that are largely aligned with major industries. The categories overlap somewhat because some specific applications apply to more than one area. However, the categories provide a useful way to organize the current and prospective applications of wireless sensor networks. Some of the application described here:[15]

1. Area monitoring
2. Environmental monitoring
3. Greenhouse monitoring
4. Landslide detection
5. Industrial monitoring
6. Machine health monitoring
7. Water/Wastewater monitoring
8. Landfill ground well level monitoring and pump counter
9. Agriculture
10. Fleet monitoring

Security is sometimes viewed as a standalone component of a system's architecture, where a separate module provides security. This separation is, however, usually a flawed approach to network security. To achieve a secure system, security must be integrated into every component, since

components designed without security can become a point of attack. Consequently, security must pervade every aspect of system design. Security in WSN is indeed a problem if you view its use for critical systems. Security must be considered in design time [57], in view of the comprehensiveness of the system and taking into account the particularities of technology, and the environments where they are implemented. It should examine the chances of triggering attacks on these networks and the impact of potential types of attacks that represent the model of adversary [23]. This analysis should be made taking into account the protocol stack [23] and associated services to software [22], [19], [20], [27] that runs on each node, since each layer services and protocols can be vulnerable to such attacks.

In the usual approach and a platform for a generic node of a WSN,each node has a minimalist stack of protocols and services, for comparison with a battery attached to a computer network standard (eg, TCP / IP or OSI) . The limitation imposed by the size and capabilities of operation does not allow architecture to be very ambitious and, secondly, the WSN generally have a vocation or oriented to specific applications, which affect the services that should be supported in the stack.

Layers of operation of a sensor node are essentially five [23]: physical layer, data link layer, network layer, transport layer and application layer. However, in most cases, the transport layer data and functionality inherent in the network layer are designed more or less specific in view of the characteristics of individual applications. On investigation, there is still that the data link layer (MAC level protocols and data-link) were the subject of several proposals, different variants that may have particular advantages, given the operation requirements of the applications. Some authors have been designing algorithms to minimize the impact of the routing attacks during the operation of WSN. These algorithms pretend to ensure some basic security properties (e.g., confidentiality, integral to the integrity, authentication, and detection of illegal retransmission of data). Nevertheless, it should consider other types of attacks specifically associated with the support of forwarding data on the network. Different routing protocols in secure WSN address only some of these types but generally do not include countermeasures against all global.

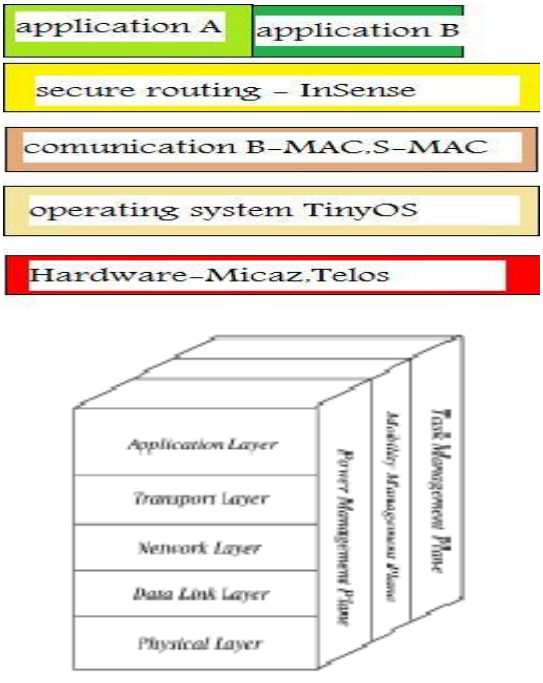

Figure 1. Stack and services protocol stack of a WSN

In this paper we designed and developed an innovative simulation system. This system should allow systematic study of routing protocols, designed to be safe, and should possess, in particular, the following features:

• Interface for visualization and network configuration information with the simulation parameters and information of each node (for example, its energy state);

• Implementation of a model that allows to extract energy consumptions at different times of operation: normal operation and determined attack before the operation;

• Model customizable generation of topologies, which can be defined as: distribution random distribution grid, distribution controlled (structured);

• Mechanism of release of failures / attacks on the network. With this mechanism aims to allow the study of the behaviors of protocols against the possibility of introducing attacks typified.

• Utilities collection of simulation data in real time and deferred time, allowing the extraction of measurements related to important properties as con-terms of energy, latency, reliability, accuracy and correctness of the protocol events, providing them graphically.

II. WSN ARCHITECTURE

In a typical WSN we see following network components [1]

1. Sensor motes (Field devices) – Field devices are mounted in the process and must be capable of routing packets on behalf of other devices. In most cases they characterize or control the process or process equipment. A router is a special type of field device that does not have process sensor or control equipment and as such does not interface with the process itself.

2. Gateway or Access points – A Gateway enables communication between Host application and field devices.

3. Network manager – A Network Manager is responsible for configuration of the network, scheduling communication between devices (i.e., configuring super frames), management of the routing tables and monitoring and reporting the health of the network.

4. Security manager – The Security Manager is responsible for the generation, storage, and Management of keys.

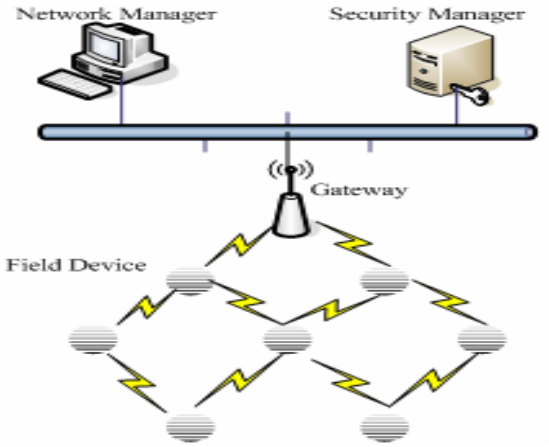

Figure 2. WSN Architecture

III. General Security Requirements in Wireless Sensor Networks

Because of the nature of wireless communications, resource limitation on sensor nodes, size and density of the networks, unknown topology prior to deployment, and high risk of physical attacks to unattended sensors, it is a challenge to provide security in WSNs. The ultimate security requirement is to provide confidentiality, integrity, authenticity, and availability of all messages in the presence of resourceful adversaries. To provide secure communications for the WSNs, all messages have to be encrypted and authenticated. Security attacks on information flow can be widespread. Modification of information is possible because of the nature of the wireless channels and uncontrolled node environments. An opponent can use natural impairments to modify information and also render the information unavailable. Security requirements in WSNs are similar to those of wireless ad hoc networks due to their similarities.[3]

***Basic Security Services*:**

Some security services have been developed for the WSN in order to ensure security in communication (eg encryption, signatures, digests). These services allow the system architect to focus on other issues related to the behavior of the protocols against attacks, eg intrusion. We present below some of the more common services that represent the basic security architecture for WSN:

***A. TinySec [20*]:** It is architecture for TinySec level protection of data binding in WSN. The main objective is to provide an adequate level of security with minimal resource consumption. The security services available are: authentication data and confidentiality. Does not implement any mechanism to ensure the freshness of the messages, making it vulnerable to attacks illicit relay.

B. MiniSec [4]: Minisec is a network layer designed to have low-energy (better than TinySec) and high security. One of the main characteristics which make it more efficient way is to use the Offset Codebook (OCB) for encryption of blocks. Thus, it is possible in a single pass, authenticate and encrypt the data without increasing the ta-morning post, contributing to lower power consumption. This architecture has two operating modes: a communication-oriented uni-cast (MINISEC-U) and one for communication broadcast (MINISEC-B);

C. SPINs A set of security protocols, consisting of two main components-parent: SNEP 6 [27] and mTESLA [27], 46]. The SNEP generate different encryption keys that are derived from a master key, shared between two nodes, with a message counter to ensure the freshness of each message. The second component, the mTESLA is an authentication service for broadcast, that avoids the use of more stringent mechanisms of asymmetric encryption using symmetric encryption, logging messages with a CMAC;

D. Standard IEEE802.15.4 [7]: This standard defines the physical layer specification and control access through the personal networks of low power (LRPAN 8). It focuses primarily on communication between devices over relatively short distances without the need for a infrastructure support, exploring the minimum energy consumption.

In this, Each device maintains a list of control ac-sos (ACL) of trusted devices, filtering out unauthorized communications after that data encryption, a cryptographic key shared between those involved in communication then Ser-bloom integrity of each frame, each frame adding a Message Integrity Code (MIC) , and finally ensuring the freshness of messages (Sequential Freshness), using counters and key frames.

E. ZigBee [5]: With the 802.15.4 standard, geared to the two lower layers of the protocol stack of WSN, ZigBee standard defines the specifications for the network layer and application. Already incorporates some security services, including: i) Freshness keeping counters associated with each session key, they are restarted on every change of key; ii) Integrity, with options for message integrity ranging from 0 to 1[21] bits verification; iii) Authentication, network level and the level of data connection, and iv) confidentiality, with the AES algorithm with 1[21] bits. This architecture uses the concept of trusted center for management of network security, implementing a ZigBee network coordinator. This, believed by all network nodes, can perform three functions: i) Authentication of us involved in the network, ii) maintenance and key distribution, iii) the safety point-to-point between network nodes.

Adversary Model: Adversary model play an important role in secure system it identify the characteristics and capabilities of the attackers and the attacks that they can trigger the network. Following are the type of opponent that informs this work.

1. ***Model of Dolev-Yao:*** One of the most popular models of adversary when it comes to formal analysis of secure protocols is the Dolev-Yao model [21]. In this model, it is considered that the network is the opponent on the field which can be extract, reorder, forward, change and deletes the messages moving between any two

legitimate nodes. With this assumption, it is understood therefore that the opponent takes the message and, therefore, adopts an attack from the man-in-the-middle [11] with misconduct. This operation, we mean, not compared to the intrusion but the interception of
messages and can be mitigated by using encryption mechanisms.

The types of attack considered by the model of Dolev-Yao adversary is instant cited by the standard X800, which aims to standardize a security architecture for the OSI model , through a systematic approach to the design of secure systems. This standard considers security in three aspects: attack, security service and mechanism [11]. The former refers to the form used to compromise a system, for example, changing or having unauthorized access to data in the system. The second aspect considered is the security mechanisms, which are understood as the process that allows detecting, preventing or recovering from an attack on security (eg encryption, access control, digital signature). Finally, the third aspect that defines the services, using one or more mechanisms for security, enable resist attacks on a particular source of information, either during processing, either during the communication.

2. ***Intrusion Model in WSN***

Whereas the study of security in WSN, and given its natural exposure, particularly physics, placing each sensor within reach of an opponent, it becomes relevant to the con-side ration of new models of opponent. Each network may consist of thousands of sensors and each of these sensors is a possible point of attack. This attack can be typified as intrusion or seizure. Such attacks can be triggered from the MAC level to the level of physical intrusion. In the latter, a player captures one or more external sensors legitimate and discovers the secrets of cryptography. This allows you to replicate the secrets to malicious souses sensors, inserted them into the network so that, acting in coordination, can compromise the network. Achieved the intrusion, the attacker can induce sensors legitimate misconduct based on false information introduced by malicious sensors, influencing the referral process. These attacks are difficult to detect, since the autonomous nature of the WSN cannot distinguish between a wrong behaviors of a fault.

Byzantine Model:

The model of Byzantine opponent's attacks by intrusion has some similarities with the so-called Byzantine failures [23], which are characterized as arbitrary failures with which a system is not at the outset, and prepared to handle it, demo result in unexpected behavior. Applying this fact to the WSN, it is difficult to detect the introduction of malicious nodes, autonomous or replicated from one node that has been compromised. However, some authors [23] have been working on this prized on in order to acquire the routing algorithms with mechanisms to detect the replication of malicious nodes in a WSN. To deal with attacks behaviors Byzantines, it resorts to probabilistic mechanisms that, although they may not completely mitigate the attack, increase resiliency and occasionally make an attack on a lesser evil, defining how far the network can be compromised in order to still ensure the reliability necessary for its operation.

IV. OSI LAYER WISE THREATS AND COUNTER MEASURES

Following are the some of the known threats and countermeasures classifying in different OSI layers[1]

Physical Layer: In Table 1, we describe Physical Layer Threats & Countermeasures in case of Wireless Sensor Network.

Threat	Countermeasures
Interference	Channel Hopping and Blacklisting
Jamming	Channel Hopping and Blacklisting
Sybil	Physical Protection of devices
Tampering	Protection and charging of Key

Table 1: Physical Layer Threats and Counter measures

Data-link Layer: In Table 2, we describe Data-Link Layer Threats & Countermeasures in case of Wireless Sensor Network.

Threat	Countermeasures
Collision	CRC and Time Diversity
Exhaustion	Protection of network ID and other information that is required to joining device
Spoofing	Use different path for re-sending the message
Sybil	Regularly Changing of key
De-synchronization	Using different neighbors for time synchronization
Traffic analysis	Sending of dummy packet in quite hours; and regular monitoring WSN network
Eavesdropping	Key protects DLPDU from Eavesdropper

Table 2. Data-link Layer Threats and Countermeasures

Network Layer: In Table 3, we describe Network Layer Threats & Countermeasures in case of Wireless Sensor Network.

Threat	Countermeasures
Wormhole	Physical monitoring of field devices and regular monitoring of network using source routing.Monitoring system may use packet Leatch techniques.
Selective Forwarding	Regular network monitoring using source routing
DOS	Protection of network specific data like Network ID etc. Physical protection and inspection of network.

Sybil	Resetting of devices and changing of session keys.
Traffic Analysis	Sending of dummy packet in quite hours and regular monitoring WSN network.
Eavesdropping	Session keys protect NPSU from Eavesdroppers.

Table 3: Network Layer Threats and Countermeasures

While there are attacks that can be directed to any of the cell layers of the WSN, Here we broadly describe the attacks related to the network layer, responsible for forwarding data.

A. Hello Flood attack

Many protocols require nodes to broadcast HELLO packets to announce themselves to their neighbors, and a node receiving such a packet may assume that it is within (normal) radio range of the sender. This assumption may be false: a laptop-class attacker broadcasting routing or other information with large enough transmission power could convince every node in the network that the adversary is its neighbor and begin exchanging information with the nodes.

Counter measures: The simplest defense against HELLO flood attacks is to verify the bi directionality of a link before taking meaningful action based on a message received over that link. The identity verification protocol is sufficient to prevent HELLO flood attacks. Not only does it verify the bidirectional link between two nodes, but even if a well-funded adversary had a highly sensitive receiver or had wormholes to a multiple locations in the network, a trusted base station that limits the number of verified neighbors for each node will still prevent HELLO flood attacks on large segments of the network when a small number of nodes have been compromised.

B. Sinkhole (Black hole) and wormhole attack

Sinkhole attacks typically work by making a compromised node look especially attractive to surrounding nodes with respect to the routing algorithm and lure nearly all the traffic from a particular area through a compromised node, creating a metaphorical sinkhole with the adversary at the center. Because nodes on, or near, the path that packets follow have many opportunities to tamper with application data, sinkhole attacks can enable many other attacks (selective forwarding, for example).

In the wormhole attack, an adversary tunnels messages received in one part of the network over a low latency link and replays them in a different part. An adversary situated close to a base station may be able to completely disrupt routing by creating a well-placed wormhole. An adversary could convince nodes who would normally be multiple hops from a base station that they are only one or two hops away via the wormhole. This can create a sinkhole: since the adversary on the other side of the wormhole can artificially provide a high-quality route to the base station, potentially all traffic in the surrounding area will be drawn through her if alternate routes are significantly less attractive.

Counter measures: Wormhole and sinkhole attacks are very difficult to defend against, especially when the two are used in combination. Wormholes are hard to detect because they use a private, out-of-band channel invisible to the underlying sensor network. Sinkholes are difficult to defend against in protocols that use advertised information such as remaining energy or an estimate of end-to-end reliability to construct a routing topology because this information is hard to verify. Routes that minimize the hop-count to a base station are easier to verify, however hop-count can be completely misrepresented through a wormhole. When routes are established simply based on the reception of a packet as in TinyOS beaconing or directed diffusion, sinkholes are easy to create because there is no information for a defender to verify. A technique for detecting

A wormhole attack is presented in [10], but it requires extremely tight time synchronization and is thus infeasible for most sensor networks. Because it is extremely difficult to retrofit existing protocols with defenses against these attacks, the best solution is to carefully design routing protocols in which wormholes and sinkholes are meaningless.

C. Sybil attack

Sybil attack is defined as a "malicious device illegitimately taking on multiple identities". Using the Sybil attack , an adversary can "be in more than one place at once" as a single node presents multiple identities to other nodes in the network which can significantly reduce the effectiveness of fault tolerant schemes such as distributed storage , disparity and multipath. It may be extremely difficult for an adversary to launch such an attack in a network where every pair of neighboring nodes uses a unique key to initialize frequency hopping or spread spectrum communication. Sybil attacks also pose a significant threat to geographic routing protocols.

Counter measures: An insider cannot be prevented from participating in the network, but she should only be able to do so using the identities of the nodes she has compromised. Using a globally shared key allows an insider to masquerade as any (possibly even nonexistent) node. Identities must be verified. In the traditional setting, this might be done using public key cryptography, but generating and verifying digital signatures is beyond the capabilities of sensor nodes. One solution is to have every node share a unique symmetric key with a trusted base station. Two nodes can then use a Needham-Schroeder like protocol to verify each other's identity and establish a shared key. A pair of neighboring nodes can use the resulting key to implement an authenticated, encrypted link between them. In order to prevent an insider from wandering around a stationary network and establishing shared keys with every node in the network, the base station can reasonably limit the number of neighbors a node is allowed to have and send an error message when a node exceeds it. Thus, when a node is compromised, it is restricted to (meaningfully) communicating only with its verified neighbors. This is not to say that nodes are forbidden from sending messages to base stations or aggregation points multiple hops away, but they are restricted from using any node except their verified neighbors to do so. In addition, an

adversary can still use a wormhole to create an artificial link between two nodes to convince them they are neighbors, but the adversary will not be able to eavesdrop on or modify any future communications between them.

V. SECURE ROUTING PROTOCOLS FOR WSN

One can establish three classes of protocols [10]: those based on location, the data-centric and hierarchical. The location-based protocols use this information to make the best decisions to achieve the targets (eg, IGF [6]). The data-centric, ie exploiting the semantics of data are usually based on algorithms that perform searches launched from synchronization (eg Directed Diffusion). Finally, the hierarchical protocol, whose design is based on building groups of nodes, usually referred to as clusters (eg, LEACH), which operate on the principle of aggregation of group data and the transfer of information for us base.

Beyond these classifications, we also consider algorithms as to when they are certain routes of transferring data. They consider themselves the protocols as table-driven or on-demand. The first refers to protocols that maintain routing tables have, exchanging control messages during its operation. Thus, there is higher power consumption, due to the regular exchange of messages. In the second case, on-demand protocols, routes are determined in each sending message. Although cause some overhead in each transmission, eventually offset more mobile and networking events with more widely spaced.
Many routing protocols for WSN have not been designed taking into account the factor of safety. Instead, they wanted to adapt to environmental applications and the characteristics and capabilities of the WSN. However, when it intends to extend its use to other areas, whose safety is essential, these concerns increase, since the security mechanisms involve a direct increase in computing and an increase in the cost of communication, reflected in the autonomy of sensors.

Following are the some secure routing protocols in WSN designed to cover the entire spectrum of the theme of this work.

1. Secure Implicit Geographic Forwarding (SIGFE): One way to address the development of secure routing protocols is to implement security mechanisms in existing protocols, but not safe. One such case is the routing algorithm Implicit Geographic Forwarding (IGF) [6] which gave rise to a safe implementation: SIGFE the IGF is a protocol on-demand, based on the location that is not keeping the state over its operation, makes it not necessary to know the network topology or the presence of other nodes. Its non-deterministic routing is already a safety mechanism against certain attacks, but it is by no means sufficient to maintain an application with safety requirements, to perform in critical environment.

The operation of IGF protocol environment is defined by the coordinates that enables each node to know exactly its location. With the aggregation network level and level 10 in a single MAC protocol Network / MAC, is possible [6], when it sent the packet, determine the next best candidate to route data. The protocol starts with the source to send a message of type Open Request To Send (ORTS) to the neighborhood (with the location and destination). Each node which is valid in the sextant 11 starts a timer for CTS (Clear To Send) inversely proportional to certain parameters (distance to the origin, existing energy and perpendicular distance to the destination), favoring nodes with better conditions. When the timer expires, a message is sent to CTS, which, when received, initiate the sending of messages of type DATA from the source. As this protocol does not maintain state, weather changes in network topology. The fact of choosing the next node in each shipment is a mechanism for fault tolerance that, in case of attack, the damage confined to the vicinity of the compromised node.

Centered at the origin, destination-oriented and determined by each node, based on your location SIGFE operation of the protocol [12] the introduction of security mechanisms in an existing protocol includes an extra burden on their operation. However, the protocol SIGFE [12] seeks to maintain a good performance and a high success rate for delivery of messages, even during an attack. One of the features of this protocol is that it is configurable and, as such, allows adjusting the security mechanisms to the level of threat. SIGFE presents three extensions to the protocol IGF [6], allowing the gradual evolution of a secure protocol, stateless, to a secure protocol, maintaining state, and, thus, heavier and more demanding in resources.

The first extension is the simplest and less demanding on resources, SIGFE-0. Continues to maintain the state and not be non-deterministic. However, do not succumb to the minutes of quos rushing type [[26]], not to issue shortly to the first node that will send a CTS. Instead, it maintains a set of possible candidates for next node. The extent intermediate SIGFE-1, already has been, but at the local level, may be with these reputation lists of their neighbors in order to better choose the next node. Finally, and since it is already a protocol more robust, but more demanding, SIGFE-[2] shares the state with its neighbors. Allows you to use cryptographic mechanisms to ensure integrity, authenticity, confidentiality and freshness. Accumulates the security properties of previous extensions: SIGFE SIGFE-0 and-1.

2. Intrusion-tolerant routing protocol for Wireless Sensor Networks (InSense)

This protocol [8] was designed with a view to intrusion tolerance and, as such, he tackles one of the types of adversary model advocated in this work. To meet this objective, we identified two types of attacks: denial of service attacks [9] and bind to the quos-forwarding. The protocol assumes the existence of a base station, establishing itself as a reliable censer who share symmetric encryption keys to each of network nodes. This feature allows, in case of compromise of a node, the attacker will have access to more than one key secure network, isolating, somehow the attack.

The use of redundant paths can increase the

resilience to attackers undetected, just that there is only one way without the interposition of attackers, so that messages arrive at their destination without being compromised. Note that in this protocol, it is not possible direct communication between network nodes, without that does not pass by the base station. The role of the protocol in terms of secure routing is played by the station base. One of the advantages mentioned by the authors, is the reduction of computations in the network nodes (eg for key generation, construction of routing tables), whose limitations are well known. The formation of routing tables is divided into three phases: Route Request (route request) Collection of data routing; propagation routes. The first phase corresponds to transmission by the base station, a message intended for all network nodes in order to obtain data on the neighborhoods. In a second phase, each node sends to its neighbor to the base station. Finally, after the base station to treat all information collected, are prepared routing tables. The tables are then propagated to each node, continuing with the routing of data, based on tables received.

3. Secure Sensor Network Routing: Clean-slate approach

The Clean-Slate algorithm [13] was designed from the outset, consistently, with characteristics of security. It is oriented point-to-point between network nodes in order to strength even in the presence of an attack (active attack). It is classified as a table-driven protocol. Operation of Protocol Each sensor network receives a globally unique identifier, a certificate signed by a CA network (AR), the public key of this entity and a set of values (challenges) based on a function of dispersion had a sensor (one-way hash function). In this protocol, one can identify the three phases of operation: network planning, establishment and maintenance of the paths of the routes.

The protocol provides the routing tables and dynamic addresses (from transformed variable) for each node using a recursive algorithm for clustering, which performs in a deterministic way, in a topology. The groups are formed recursively and hierarchically, until the network form a single group. In each fusion is added a bit (0 / 1) to the left, which will distinguish the address of each node. Within a group, communication is done using authenticated broadcast, inspired by the protocol mTESLA[27],This algorithm incorporates mechanisms to detect incorrect behavior of the nodes, for example, if they wish to assume multiple identities (Sybil [9]). This mechanism is triggered after the formation of groups, with each node to advertise its address for the neighbors, applying an algorithm to detect replication of us[22].Another mechanism for the detection of incorrect formation of groups is the use of Grouping Verification Trees (GVT), based on scales of dispersal that provide authentication at leaf level, using the root for certification. Each node has a GVT, allowing verifying any communication exchanged with other network nodes.

During the maintenance phase of routes and routing, the algorithm incorporates operations for treating the input and output nodes. By detecting the output of another, a demand node in one of his neighbors, a new border node, allowing it to reach the group accessible to the node before it came out. The definition of seasons (epochs) allows, after some time, the clustering algorithm will be repeated to include new nodes. Regarding the routing, the protocol uses multiple routes, so that affected areas can bypass the network. The malicious nodes are removed from the algorithm, by using a technique called Honeybee. Corresponds to the following: when a malicious node (replicated or not) is detected, the network is flooded with a package that indicates that the attacker must be removed from the tables and, in the case of a replication, the replicated node is leaving the auto scarification network.

Briefly, the clean-slate protocol incorporates three concepts for the design of secure routing protocols: prevention (authentication), resilience (multiple routes) and detection/ recovery (GVT /Honeybee). Implements them simultaneously, unlike what happens with some protocols that implement only one of these concepts. It is therefore an underlying protocol, suitable for the comparative study with other protocols.

Thus, in Table below, are marked with symbol X and Y attacks defended by each protocol studied, of which those marked with × not advocate or do so only under special conditions. The protocol SIGFE distinguishes itself from other protocols studied, particularly for its origin (length IGF) and be based on location. This feature is specific for certain applications and requires the existence of specialized devices in the motes. In addition, it is particularly suitable for monitoring events occurring spaced in time. By configurable, makes suits depending on the degree of threat, increasing operating costs with increased threat. The protocols and InSense Clean-Slate, which will be used as proof of concept in preparation the dissertation, do not require knowledge of location, reducing the complexity network platform. These protocols, due to the characteristics that define them, are excellent candidates for a comparative study. One characteristic that distinguishes them is the use base station as a core unit of routing, by InSense. In contrast, Clean-slate approach is completely distributed. The question that arises in InSense, concerns itself mostly with the impact on energy consumption of the nodes near (to one hop) of the base station, since this will forward all traffic on the network.

Both protocols implement resilience to intrusion. One difference is that the Clean-Slate has a preventive action, corresponding to the detection of malicious nodes (replicated). Furthermore, routing is multi-route, which minimizes the impact of the intruder that resist detection. In the case of InSense, there is only one mechanism redundant multi-route. Observe that the authors of the Clean-Slate made a comparative study, theoretical, for InSense to (because it already exists.) The implementation of these two algorithms, a same basic simulation will verify that the observations meet the authors' conclusions. This comparative study will be of major importance for the study of other protocols that arise in academia, related to issues of security in routing of data in WSN. In relation to attacks that can be directed to each of the

protocols, it is important to highlight the Sybil attack, as a case difficult to resolve when it derives from an intrusion, in which an attacker has obtained the necessary keys to being

PROTOCOLS	SIGF	INSENS	Clean Slate
Info-fake	Y	Y	Y
rushing	Y	Y	Y
HELLO flooding	Y	Y	Y
sinkhole	x	x	x
wormhole	x	x	x
Sybil	Y	Y	Y
Black hole	Y	Y	Y
Intrusion replication	x/x	x/x	x/x

Table 4:Table of Routing Protocols vs Attacks

able to advertise on any of the identities he has assumed. Thus, resistance to this attack by the protocols studied does not take into account the mode of intrusion, because assumes that each attacker has all the necessary keys to authenticate with false identities and, as such, can be detected.

VI. IMPEMENTATION AND RESULT OF SECURE ROUTING PROTOCOLS IN WSN

Earlier this stage it will be necessary to re-intensify the operation of each algorithm to implement, understand and identify each mechanism / technique specified, so that it can, where possible, to generalize operations or interfaces in order to reuse for other algorithm. Thus, this phase will require a learning / knowledge of each algorithm, also contributing to the expertise in this field.

Using the tools provided by the platform, it should be possible at the end of implementation, to systematize the simulations, in order to extract results. These results, by itself, the algorithms must characterize safety and whether the correction certain parameters, namely:

- protocol correct,
- analysis of energy consumption;
- reliability and delivery of messages;
- the correction of events;
- Latency.

This phase contributes also to measure the usability of the platform in terms of assessment / comparison secure routing protocols in WSN.

Analysis: This activity reflects the additional review of the literature with a double Objective To deepen the problem under study and evaluate the simulator. It starts also the design and specification of the platform, consisting of the formal definition of algorithms, interfaces and interaction model components of the platform. During the development phase, this activity will be revisited in order to refine / update the specification of the platform, including by the use of modeling tools for object-oriented systems (UML).

Development: activity reflects the design and implementation of the architecture platform,, in which each component corresponds the following tasks: Integration of Simulation Base Configuration Module , Management module topologies, Management module Energy , Module View and Module Injection Attack.

Proof of Concept This activity matches the implementation of a basic algorithm (eg flooding without repetition of messages sent) and routing algorithms Insurance proposed: InSense and Clean-Slate. This implementation should be preceded by a more detailed study of the peculiarities of each. Consequently, each protocol will be subject to a type of attack, which will assess their behavior in order to check the properties, identified earlier as important for the analysis of a secure routing protocol in WSN.

Assessment: This activity calls for the evaluation of the protocols implemented, using the tools platform, This assessment will also draw conclusions about the usability of the platform and the objectives required. These are the ability to study routing protocols in WSN, in general, and particularly those with security concerns.

Report: this activity corresponds to writing the dissertation and should start as soon as complete the process of specifying the platform, allowing the realization of the model objects. This phase may take place in parallel with the assessment activity and eventually, with the proof of concept.

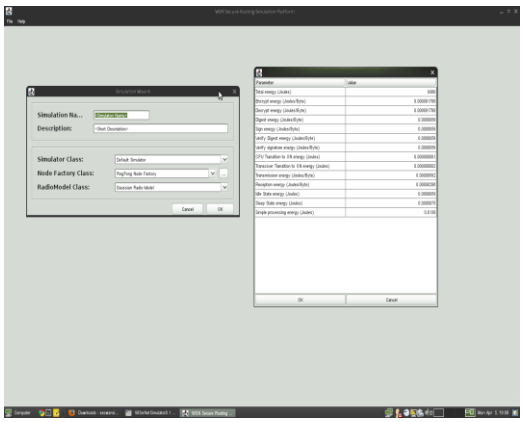

Figure 3.OUT PUT 1

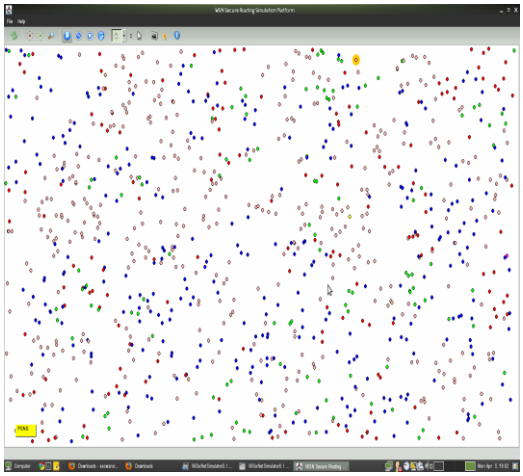

Figure 4.OUT PUT 2

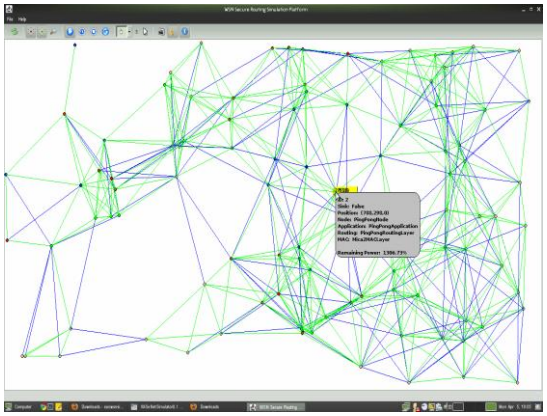

Figure 5.OUT PUT 3

VII. Conclusion and Future Work

In this work we have been able to evaluate the security conditions and robustness criteria of routing protocols for WSN. We have been able to assess and compare the security protocols using a simulation platform in closed-to-real operating conditions. An evaluation of the security and intrusion tolerance of the protocol has been made.

Dolev-Yao adversary model used here successfully simulates the attacks on the communication channel. This has helped us to design specific counter-measures against such attacks.

The design of the simulation environment is the major contribution of this project, since many available simulations systems do not have some of ITS features incorporated here. This will be a great help in the design of secure routing protocols and future work are:

- MAC-level implementation lifecycle Sensor.
- Definition of graphical display of results, energy.
- Data collection for evaluation Offline.
- Possibility of distributed simulation with submission of jobs.
- Evaluation of the usability of the API to develop new protocols.
- Development of a cipher suite out-of-the-box.

VIII. References

[1] WIRELESS SENSOR NETWORK SECURITY ANALYSIS, Hemant Kumar Kalita1 and Avijit Kar[19], International Journal of Next-Generation Networks (IJNGN),Vol.1, No.1, December 2009

[2] Wireless Networks. Security Vulnerabilities In Wireless Sensor Networks: A Survey. Journal of Information Assurance and Security, 5([19]010):031–044, 2009.

[3] Security Issues in Wireless Sensor Networks Zoran S. Bojkovic, Bojan M. Bakmaz, and Miodrag R. Bakmaz, INTERNATIONAL JOURNAL OF COMMUNICATIONS
Issue 1, Volume 2, 2008

[4] Mark Luk, Adrian Perrig, Ghita Mezzour, and Virgil Gligor. MiniSec: a secure sensor network communication architecture. pages 479–488, Cambridge, Massachusetts, USA, 2007. ACM.

[5] Paolo Baronti, Prashant Pillai, Vince W.C. Chook, Stefano Chessa, Alberto Gotta, andY. Fun Hu. Wireless sensor networks: A survey on the state of the art and the 80[19].15.4and ZigBee standards. Computer Communications, 30(7):1655–1695, May 2007.

[6] M. Blum, Tian He, Sang Son, and John A Stankovic. IGF: a State-Free robust communication protocol for wireless sensor networks.

[7] IEEE Standard for Information Technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - specific requirement Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specificationsfo, 2007.

[8] Jing Deng, Richard Han, and Shivakant Mishra. Insens: Intrusion-tolerant routing for wireless sensor networks. Comput. Commun., [292:216–230, 2006.

[9] Fei Hu and Neeraj K. Sharma. Security considerations in ad hoc sensor networks. Ad Hoc Networks, 3(1):69–89, January 2005.

[10] Kemal Akkaya and Mohamed Younis. A survey on routing protocols for wireless sensor networks. Ad Hoc Networks, 3(3):325–349, May 2005.

[11] William Stallings. Cryptography and Network Security (4th Edition). 2005

[12] Anthony D. Wood, Lei Fang, John A. Stankovic, and Tian He. SIGF: a family of configurable, secure routing protocols for wireless sensor networks. pages 35–48, Alexandria, Virginia, USA, 2006. ACM.

[13] Bryan Parno, Mark Luk, Evan Gaustad, and Adrian Perrig. Secure sensor network routing: a clean-slate approach. In CoNEXT '06: Proceedings of the 2006 ACM CoNEXT conference, pages 1–13, New York, NY, USA, 2006. ACM.

[14] B. Parno, A. Perrig, and V. Gligor. Distributed detection of node replication attacks in sensor networks. pages 49–63, 2005.

[15].Wireless Sensor Systems and Networks: Technologies, Applications, Implications and Impacts *David J. Nagel Professor of Engineering and Applied Science The George Washington University*

[16].Wireless Sensor Networks: Principles and Applications *Chris Townsend, Steven Arms MicroStrain, Inc.*

[17].Adrian Perrig and Haowen Chan. Security and Privacy in Sensor Networks

[18].Chris Karlof and David Wagner. Secure routing in wireless sensor networks: attacks and countermeasures. Ad Hoc Networks, 1(2-3):293–315, September 2003.

[19].The contiki operating system - home. _ HYPERLINK "http://www.sics.se/contiki/" _http://www.sics.se/contiki/_.

[20].Chris Karlof, DavidWagner, and Naveen Sastry. TinySec: a link layer security architecture for wireless sensor networks. pages 162–175, Baltimore, MD, USA, 2004. ACM.

[21].D. Dolev and A. Yao. On the security of public key protocols.

Information Theory, IEEETransactions on, 29(2):198–208, 1983

[22]. TinyOS community forum || an open-source OS for the networked sensor regime.
http://www.tinyos.net/.

[23]. I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci. Wireless sensor networks:a survey. Computer Networks, March 2009.

[[27]]. Adrian Perrig, Robert Szewczyk, Victor Wen, David Culler, and J. D. Tygar. Spins: Security protocols for sensor networks.

[26]Yih-Chun Hu, Adrian Perrig, and David B. Johnson. Rushing attacks and defense in wireless ad hoc network routing protocols. In WiSe '03: Proceedings of the 2nd ACM
workshop on Wireless security, pages 30–40, New York, NY, USA, 2003. ACM.

[27]Adrian Perrig, Robert Szewczyk, Victor Wen, David Culler, and J. D. Tygar. Spins: Security protocols for sensor networks. In Wireless Networks, pages [23]9–199, 2001.