M. L.S. N. S. Lakshmi, S.Gopi Krishna / International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com
Vol. 2, Issue4, July-August 2012, pp.1462-1475

A Quick Over View Of Wireless Sensor Networks, Routing Protocols And Security Constraints

M. L.S. N. S. Lakshmi *, S.Gopi Krishna**

*(Department of Electronics, KONERU LAKSHMAIAH University, Vaddeswaram.,Vijayawada,Andhra Pradesh,India

** (Department of Electronics, KONERU LAKSHMAIH University,Vaddeswaram,Vijayawada,Andhra Pradesh,India.

ABSTRACT

The recent advances and the convergence of micro electro-mechanical systems technology, integrated circuit technologies, microprocessor hardware and nano technology, wireless communications, Ad-hoc networking routing protocols, distributed signal processing, and embedded systems have made the concept of Wireless Sensor Networks (WSNs) and the advances in wsns have led to many protocols specifically designed for sensor networks. Sensor network nodes are limited with respect to energy supply, restricted computational capacity and communication bandwidth. Most of the attention, however, has been given to the routing protocols since they might differ depending on the application and network architecture. To prolong the lifetime of the sensor nodes, designing efficient routing protocols is critical. Even though sensor networks are primarily designed for monitoring and reporting events, since they are application dependent, a single routing protocol cannot be efficient for sensor networks . This paper surveys and gives explanatory details about wsn (wireless sensor networks) ,its protocols and security constraints and protocols for restriction of unauthorized authentication recent routing protocols for sensor networks and presents a classification for the various approaches pursued.

Keywords – sensor network,multi hop,routing protocol,security,data aggregation,centralized,.localised

1. INTRODUCTION

Wireless sensor networks (WSNs) are being used in a wide variety of critical applications such as military and health-care applications. WSNs are deployed densely in a variety of physical environments for accurate monitoring. Therefore, order of receiving sensed events is important for correct interpretation and knowledge of what actually is happening in the area being monitored. Similarly, in intrusion detection applications (alarm application), response time is the critical performance metric. On detection of intrusion, alarm must be signaled within no time. There should be a mechanism at node for robust communication of high priority messages. Once deployed, the sensors are expected to self-configure into a wireless network. Sensor networks consist of a large number of sensor nodes that collaborate together using wireless communication and asymmetric many-to-one data. Indeed, sensor nodes usually send their data to a specific node called the sink node or monitoring station, which collects the requested information. The limited energy budget at the individual sensor level implies that in order to ensure longevity, the transmission range of individual sensors is restricted, perhaps of the order of a few meters. In turn, this implies that wireless sensor networks should be multihop. An important difference between wireless sensor networks and conventional networks is that sensor nodes do not need node addresses (e.g., medium-access control (MAC) address and Internet protocol (IP) address). In conventional networks (e.g., Internet), the node address is used to identify every single node in the network. Various communication protocols and algorithms are based on this low-level naming. However, wireless sensor networks are information-retrieval networks, not point-to-point communication networks. That is, wireless sensor network applications focus on collecting data, rather than on providing communication services between network nodes. Node address is not essential for sensor network applications. Wireless sensor networks are a special case of ad hoc networks. However, there are several major differences between wireless sensor networks and ad hoc networks.

2. ARCHITECTURE

A sensor network is a network of many tiny disposable low power devices, called nodes, which are spatially distributed in order to perform an application-oriented global task. These nodes form a network by communicating with each other either directly or through other nodes. One or more nodes among them will serve as sink(s) that are capable of communicating with the user either directly or through the existing wired networks. The primary component of the network is the sensor, essential for monitoring real world physical conditions such as

sound, temperature, humidity, intensity, vibration, pressure, motion, pollutants etc. at different locations. The tiny sensor nodes, which consist of sensing, on board processor for data processing, and communicating components, leverage the idea of sensor networks based on collaborative effort of a large number of nodes. Figure 1 shows the structural view of a sensor network in which sensor nodes are shown as small circles. Each node typically consists of the four components: sensor unit, central processing unit (CPU), power unit, and communication unit. They are assigned with different tasks. The sensor unit consists of sensor and ADC (Analog to Digital Converter). The sensor unit is responsible for collecting information as the ADC requests, and returning the analog data it sensed. ADC is a translator that tells the CPU what the sensor unit has sensed, and also informs the sensor unit what to do. Communication unit is tasked to receive command or query from and transmit the data from CPU to the outside world. CPU is the most complex unit. It interprets the command or query to ADC, monitors and controls power if necessary, processes received data, computes the next hop to the sink, etc. Power unit supplies power to sensor unit, processing unit and communication unit. Each node may also consist of the two optional components namely Location finding system and Mobilizer. If the user requires the knowledge of location with high accuracy then the node should pusses Location finding system and Mobilizer may be needed to move sensor nodes when it is required to carry out the assigned tasks.

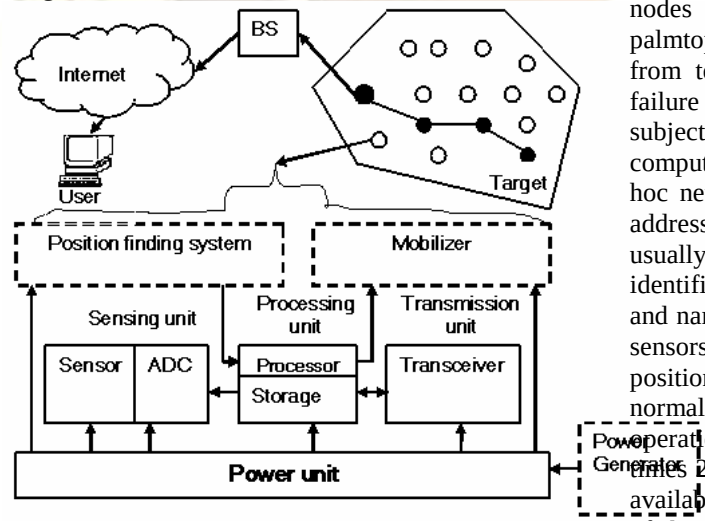

Fig 1: Structural view of sensor network

Instead of sending the raw data to the nodes responsible for the fusion, sensor nodes use their processing abilities to locally carry out simple computations and transmit only the required and partially processed data. The sensor nodes not only collect useful information such as sound, temperature, light etc., they also play a role of the router by communicating through wireless channels under battery-constraints. Sensor network nodes are limited with respect to energy supply, restricted computational capacity and communication bandwidth. The ideal wireless sensor is networked and scalable, fault tolerance, consume very little power, smart and software programmable, efficient, capable of fast data acquisition, reliable and accurate over long term, cost little to purchase and required no real maintenance.

The basic goals of a WSN are to:

- determine the value of physical variables at a given location,
- detect the occurrence of events of interest, and estimate parameters of the detected event or events,
- classify a detected object, and
- track an object.

Thus, the important requirements of a WSN are:

- use of a large number of sensors,
- attachment of stationary sensors,
- low energy consumption,
- self organization capability,
- collaborative signal processing, and
- querying ability.

3. WIRELESS SENSOR NETWORKS

To begin, the nodes of a wireless sensor network are generally densely deployed (e.g., hundreds or thousands of sensors may be placed, mostly at random, either very close or inside the phenomenon to be studied). Also, the number of nodes is typically not the same: while there are hundreds or thousands of sensors, the number of nodes (laptops, personal digital assistants (PDAs), palmtops, etc.) in an ad hoc network normally ranges from tens to hundreds. The sensors have a larger failure rate and feature lower data reliability, and are subject to stringent limitations in the energy budget, computing capacity, and memory. The nodes of an ad hoc network are normally distinguished by their IP addresses or other identifiers, while sensors are usually anonymous, lacking fabrication-time identifiers. Consequently, they are being addressed and named using various strategies that either endow sensors with temporary IDs or else rely on data or position-driven naming. While ad hoc networks normally rely on topological information in their operation (e.g., knowledge of one-hop and often times 2-hop neighbors), such information may not be available in wireless sensor networks simply because of the lack of IDs at the individual sensor level. In some cases, however, the sensors benefit from a sense of relative geographic position with respect to the monitored environment and/or with respect to a sink. Thus, positional information may be essential in some applications of sensor networks, although it may not be essential for ad hoc networks.

Depending on the application, different architectures and design goals/ constraints have been considered for wireless sensor networks. We attempt

to capture architectural design issues and highlight their implications on the network infrastructure. There are three main components in a sensor network. These are the sensor nodes, the sink, and the monitored events. Aside from the few architectures that utilize mobile sensors, most of the network architectures assume that sensor nodes are stationary. On the other hand, supporting the mobility of sinks, clusterheads (CHs), or gateways is sometimes deemed necessary. Routing messages from or to moving nodes is more challenging, since route stability becomes an important optimization factor, in addition to energy, bandwidth, and the like. The sensed event can be either dynamic or static depending on the application. For instance, in a target detection/ tracking application, the event (phenomenon) is dynamic, whereas forest monitoring for early fire prevention is an example of static events. Monitoring static events allows the network to work in a reactive mode, simply generating traffic when reporting. Dynamic events in most applications require periodic reporting, and consequently generate significant traffic to be routed to the sink.

An important design consideration is the topological deployment of nodes. This is usually application-dependent and affects the performance of the communication protocol. The deployment is either deterministic or self-organizing. In deterministic situations, the sensors are manually placed and data are routed through predetermined paths. In addition, collision among the transmissions of the different nodes can be minimized through the prescheduling of medium access. However, in self organizing systems, the sensor nodes are scattered randomly, creating an infrastructure in an ad hoc manner. In that infrastructure, the position of the sink or the CH is also crucial in terms of energy efficiency and performance. When the distribution of nodes is not uniform, optimal clustering becomes a pressing issue to enable energy efficient network operation. During the creation of an infrastructure, the process of setting up the network topology is greatly influenced by energy considerations.

Since the transmission power of a wireless radio is proportional to distance squared or even higher order in the presence of obstacles, multihop routing will consume less energy than direct communication. However, multihop routing introduces significant overhead for topology management and MAC. Direct routing would performed well enough if all the nodes were very close to the sink. Most of the time sensors are scattered randomly over an area of interest, and multihop routing becomes unavoidable. Arbitrating medium access in this case becomes cumbersome. Depending on the application of the wireless sensor network, the data-delivery model to the sink can be continuous, event-driven, query-driven, and hybrid. In the continuous-delivery model, each sensor sends data periodically. In event driven and query-driven models, the transmission of data is triggered when an event occurs or when a query is generated by the sink. Some networks apply a hybrid model using a combination of continuous, event-driven, and query-driven data delivery. The routing and MAC protocols are highly influenced by the data delivery model, especially with regard to the minimization of energy consumption and route stability. For instance, it has been concluded in that for a habitat monitoring application where data are continuously transmitted to the sink, a hierarchical routing protocol is the most efficient alternative. This is due to the fact that such an application generates significant redundant data that can be aggregated en route to the sink, thus reducing traffic and saving energy. In addition, in the continuous data-delivery model time-based medium access can achieve significant energy saving, the since it will enable turning off sensors' radio receivers. Carrier sense multiple access (CSMA) medium-access arbitration is a good fit for event-based data-delivery models, since the data are generated sporadically.

In a wireless sensor network, different functionalities can be associated with the sensor nodes. In the early work on sensor networks, all sensor nodes are assumed to be homogenous, having equal capacity in terms of computation, communication, and power. However, depending on the application a node can be dedicated to a particular special function, such as relaying, sensing, and aggregation, since engaging the three functionalities at the same time on a node might quickly drain the energy of that node. . While some networks have selected CHs from the deployed sensors in other applications a CH is more powerful than the sensor nodes in terms of energy, bandwidth, and memory. In such cases, the burden of transmission to the sensor nodes in terms of energy, bandwidth, and memory. In such cases, the burden of transmission to the sink and aggregation is handled by the CH.

4. DATA AGGREGATION IN WIRELESS SENSOR NETWORKS

When data are measured or arrive from a neighbor, the sensor needs to decide whether or not they are important enough to forward them. The coding techniques used need to minimize the number of forwarded bits. The new data may also be combined with other received data, in order to minimize the number of bits to forward. Such data aggregation (also referred to as fusion) from multiple sensors is important, because of severe energy and bandwidth limitations as well as for numerous other reasons, including reliability. The reliability of individual measurements bandwidth or delay guarantees. Therefore, the transport control protocols designed for wired networks or for other kinds of wireless networks cannot be used for wireless sensor networks. When an event occurs, there is usually a multiple correlated data flow from the event to sink.

A spatial correlation exists among the data reported. Several reports may arrive at the sink, or several reports can be combined at intermediate nodes to reduce communication (data fusion). The sink makes a decision on the event based on these reports, which has a certain degree of collective reliability. The transport- layer problem in wireless sensor networks can be defined concisely as follows: to configure the reporting rate to achieve the required event detection reliability at the sink with minimum resource utilization.

6. QUERY PROCESSING IN WIRELESS NETWORKS

In other types of networks, queries are normally address-centric in the sense that they are sent to an individual node using, for example, IP-based routing. By contrast, the anonymity of sensors suggests that in wireless sensor networks queries be either location-centric or data-centric. Queries are addressed to a geographic region rather than to individual sensors. Since, as we discussed, the sensors do not have unique IDs, routes are created based on the nature and value of data collected by sensors. An example of data-driven routing is the response to a query that is asking to report all sensor readings with temperature over 408C. Queries can be distinguished along several orthogonal axes. Spatially, queries may be global and be sent to the entire deployment area, or area-specific, in which case they are addressed to a geo casting region (where only sensors inside a geographic region are asked to report), or to multi geo casting regions (where all sensors located inside several geographic regions are asked to report). In terms of the reporting mechanism there are several possible types of queries. We only mention the following three: event-driven, on-demand, and persistent. In an event-driven query, the sensor itself decides when it has something to report (for instance, when it measures high temperature, which may indicate incipient fire). In an on demand query, the request comes from the end user via the sink. In a persistent query, the end user expresses a long-term interest in an event or a disjunction of events. The various sensors tasked with answering the persistent query report whenever a trigger event occurs during the lifetime of the interest

6. STRATEGIES OF WIRELESS SENSOR NETWORKS

There are several strategies for deploying wireless sensor networks. The sensors can be embedded in the ambient environment, be embedded in the asphalt covering streets and highways, in the walls of building, in trees, and so on. They can be placed deterministically by humans or robots, or incorporated in the paint coating walls, or deployed in a purely random fashion. Most research is devoted to random placement, where the sensors are dispersed randomly by plane, artillery, humans, or robots. Further, the initial deployment may be followed by later redeployment, as necessary. Wireless sensor network self-organization includes a time component. One aspect of the problem is the time at which each sensor starts to operate. In many protocols, there exists an implicit assumption that all sensors start to operate at the same time, which could be preprogrammed, or may be externally decided and communicated.

The later option is avoided because sensors need to be in the idle state to receive any instruction, which is much more energy-consuming compared to the sleep state (when receivers are turned off). Sensor network operation may require time synchronization (covered in Chapter 7 in this book), whether or not all sensors follow the same time or at least have synchronized time slots. Time synchronization can be provided by a global positioning system (GPS), by collaborative efforts, or can be achieved by some other means. Some applications benefit or even require that the sensory data collected by sensors be supplemented with location information, which encourages the development of communication protocols that are location aware and perhaps location dependent. The practical deployment of many sensor networks will result in sensors initially being unaware of their location: they must acquire this information post deployment.

In fact, in most of the existing literature, the sensors are assumed to have learned their geographic position. The location-awareness problem is for individual sensors to acquire location information either in absolute form (e.g., geographic coordinates) or relative to a reference point. The localization problem is for individual sensors to determine, as precisely as possible, their geographic coordinates in the area of deployment. One simple solution to the localization problem is to use a GPS, where sensors receive signals from several satellites and decide their position directly. However, for tiny sensors such direct position learning may not be possible or may not be sufficiently accurate enough (if a GPS signal is not provided with sufficient accuracy) for the assigned task. However, due to limitations in form factor, cost per unit, and energy budget, individual sensors are not expected to be GPS enabled. Moreover, in many occluded environments, including those inside buildings, hangars, or warehouses, satellite access is drastically limited. Since direct reliance of GPS is specifically proscribed, in order to obtain location awareness individual sensors exchange messages to collaboratively determine their own geographic position (absolute or relative) in the network. The vast majority of collaborative solutions to the localization problem are based on multi lateration or multiangulation. These solutions assume the existence of several anchors that are aware of their geographic position (e.gsinks or specialized

sensors that can engage in satellite communication). By exchanging messages with their neighbors, individual sensors can conceivably measure signal strengths and/or time delays in communication. Some approaches are based on hop-count distances to reference points. Sensors receiving location messages from at least three sources can approximate their own locations In some other applications, exact geographic location is not necessary: all that individual sensors need is coarse-grain location awareness. There is an obvious trade-off; coarse-grain location awareness is lightweight, but the resulting accuracy is only a rough approximation of the exact geographic coordinates. One can obtain this coarse-grain location awareness by a training protocol that imposes a coordinate system onto the sensor network. an interesting by product of such a training protocol is that it provides partitioning into clusters and a structured topology with natural communication paths. The resulting topology will make it simple to avoid collisions between transmissions of nodes in different clusters, between different paths, and also between nodes on the same path. This is in contrast with the majority of papers that assume routing along spanning trees with frequent collisions. In the training protocol the deployment area is endowed with a virtual infrastructure to make the presentation self-contained, however, we now outline the idea. The coordinate system divides the sensor network area into equiangular wedges. In turn, these wedges are divided into sectors by means of concentric circles or coronas centered at the sink. The task of training the wireless sensor network involves establishing coronas The deployment area is covered by coronas determined by concentric circles centered at the sink . Wedges: The deployment area is ruled into a number of angular wedges centered at the sink. Individual sensors can acquire the desired coarse-grain location awareness by learning the identity of the corona and the wedge to which they belong. As it turns out, the training protocol is lightweight and does not require sensors to have IDs; moreover, sensors are not aware of their neighbors within the same sector. It is worth noting that location awareness is modulo the sector to which the sensor belongs. Since accurate position information is unreliable because of shadowing, scattering, multi paths, and time synchronization problems, training provides a viable alternative.

7. COMPARISON OF MANETS AND SENSOR NETWORKS

MANETS (Mobile Ad-hoc networks) and sensor networks are two classes of the wireless Adhoc networks with resource constraints. MANETS typically consist of devices that have high capabilities, mobile and operate in coalitions. Sensor networks are typically deployed in specific geographical regions for tracking,monitoring and sensing. Both these wireless networks are characterized by their ad hoc nature that lack pre deployed infrastructure for computing and communication. Both share some characteristics like network topology is not fixed, power is an expensive resource and nodes in the network are connected to each other by wireless communication links. WSNs differ in many fundamental ways from MANETS as mentioned below.

- Sensor networks are mainly used to collect information while MANETS are designed for distributed computing rather than information gathering.
- Sensor nodes mainly use broadcast communication paradigm whereas most MANETS are based on point-to-point communications.
- The number of nodes in sensor networks can be several orders of magnitude higher than that in MANETS .
- Sensor nodes may not have global identification (ID) because of the large amount of overhead and large number of sensors.
- Sensor nodes are much cheaper than nodes in a MANET and are usually deployed in thousands.
- Sensor nodes are limited in power, computational capacities, and memory where as nodes in a MANET can be recharged somehow.
- Usually, sensors are deployed once in their lifetime, while nodes in MANET move really in an Ad-hoc manner.
- Sensor nodes are much more limited in their computation and communication capabilities than their MANET counterparts due to their low cost.

8. APPLICATIONS OF SENSOR NETWORKS

In the recent past, wireless sensor networks have found their way into a wide variety of applications and systems with vastly varying requirements and characteristics. The sensor networks can be used in Disaster Relief, Emergency Rescue operation, Military, Habitat Monitoring, Health Care, Environmental monitoring, Home networks, detecting chemical,
biological, radiological, nuclear, and explosive material etc. as summarized in table 1.

TABLE 1
SOME APPLICATIONS FOR DIFFERENT AREAS

Area	Applications
Military	Military situation awareness. Sensing intruders on basis. Detection of enemy unit movements on land and sea. Battle field surveillances
Emergency Situations	Disaster management. Fire/water detectors. Hazardous chemical level and fires.
Physical World	Environmental monitoring of water and soil. Habitual monitoring. Observation of biological and artificial systems.
Medical and health	Sensors for blood flow, respiratory rate, ECG (electrocardiogram),pulse oxymeter, blood pressure and oxygen measurement. Monitoring people's location and health condition.
Industrial	Factory process control and industrial automation. Monitoring and control of industrial equipment.
Home Networks	Home appliances, location awareness (blue tooth). Person locator.
Automotive	Tire pressure monitoring. Active mobility. Coordinated vehicle tracking.

9. ROUTING

Routing in sensor networks is very challenging due to several characteristics that distinguish them from contemporary communication and wireless ad hoc networks. First of all, it is not possible to build a global addressing scheme for the deployment of sheer number of sensor nodes. Therefore, classical IP-based protocols cannot be applied to sensor networks. Second, in contrary to typical communication networks almost all applications of sensor networks require the flow of sensed data from multiple regions (sources) to a particular sink. Third, generated data traffic has significant redundancy in it since multiple sensors may generate same data within the vicinity of a phenomenon. Such redundancy needs to be exploited by the routing protocols to improve energy and bandwidth utilization. Fourth, sensor nodes are tightly constrained in terms of transmission power, on-board energy, processing capacity and storage and thus require careful resource management. Due to such differences, many new algorithms have been proposed for the problem of routing data in sensor networks. These routing mechanisms have considered the characteristics of sensor nodes along with the application and architecture requirements. Almost all of the routing protocols can be classified as data-centric, hierarchical or location based although there are few distinct ones based on network flow or quality of service (QoS) awareness. Data-centric protocols are query-based and depend on the naming of desired data, which helps in eliminating many redundant transmissions. Hierarchical protocols aim at clustering the nodes so that cluster heads can do some aggregation and reduction of data in order to save energy. Location based protocols utilize the position information to relay the data to the desired regions rather than the whole network. The last category includes routing approaches that are based on general network-flow modeling and protocols that strive for meeting some QoS requirements along with the routing function, in this paper, we will explore the routing mechanisms for sensor networks developed in recent years. Each routing protocol is discussed under the proper category. Our aim is to help better understanding of the current routing protocols for wireless sensor networks and point out open issues that can be subject to further research.

10. ROUTING PROTOCOL

Routing protocols work on the assumption that every node is aware of its own position in the network; via mechanisms like GPS or distributed localization schemes and that the physical topology of the network is a good approximation of the network connectivity. In other words, these routing protocols assume that if two nodes are physically close to each other, they would have radio connectivity between them, which is true in most cases. Hence the protocols use node location information to route packets from source to destination. Every node having its location information is a fair assumption in most sensor networks since application data frequently needs to be annotated by location information. One big advantage of geographic routing schemes is the fact that there is no need to send out route requests or periodic connectivity updates. This can save a lot of protocol overhead and consequently, energy of the nodes. This is an important consideration for sensor networks where the network size could be on the order of thousands of nodes, but each node has extremely limited memory capacity to store routing tables.

10.1.Localized versus centralized protocols

Due to a number of factors, the topology of wireless sensor networks changes frequently and self organization must be adaptive to local changes. Centralized protocols require global network information at each sensor (sink only, respectively,

with sink making decisions) for making sensor decisions. This includes the use of topological structures, such as minimal spanning tree (MST), whose local links cannot be locally determined. There are a number of combinatorial optimization formulations of sensor network design problems with linear programming solutions. These protocols can perform well only when sensor networks are small. We do not discuss centralized approaches further, since we believe in and assume large-scale wireless sensor networks where centralized protocols do not work well. Localized protocols only require local knowledge for making decisions, and a limited (usually constant) amount of additional information (e.g., the position of the sink). Some localized protocols may require preprocessing, such as constructing a suitable topology for further operation. One typical example is setting up a cluster structure. In addition to localized protocol operation, it is also important to consider the maintenance cost of such topology. For instance, if the cluster structure is adopted, what happens when CHs move or fail? Does the update procedure remain local, and, if so, what is the quality of the maintained structure over time? Some maintenance procedures may not remain local. This happens when local change triggers message propagation throughout the network. Of course, localized maintenance is preferred, meaning that local topology changes should be performed by a procedure that always remains local, involving only the neighborhood of the affected sensors.

A number of protocols in the literature are localized, but use an excessive number of messages between neighboring sensors. For instance, some topology control and position determination protocols require over a dozen (sometimes even thousands of) messages to be exchanged between neighbors. Because of the severely limited bandwidth and energy budget and medium-access problems caused by excessive messaging, messages between neighbors to construct/maintain topology, determine position, or perform any other operation should be minimized, possibly avoided entirely .

10.2. Classification Of Routing Protocols

The design space for routing algorithms for WSNs is quite large and we can classify the routing algorithms for WSNs in many different ways. Routing protocols are classified as node centric, data-centric, or location-aware (geo-centric) and QoS based routing protocols. Most Ad-hoc network routing protocols are node-centric protocols where destinations are specified based on the numerical addresses (or identifiers) of nodes. In WSNs, no decentric communication is not a commonly expected communication type. Therefore, routing protocols designed for WSNs are more data-centric or geocentric. In data-centric routing, the sink sends queries to certain regions and waits for data from the sensors located in the selected regions. Since data is being requested through queries, attribute based naming is necessary to specify the properties of data. Here data is usually transmitted from every sensor node within the deployment region with significant redundancy. In location aware routing nodes know where they are in a geographical region. Location information can be used to improve the performance of routing and to provide new types of services. In QoS based routing protocols data delivery ratio, latency and energy consumption are mainly considered. To get a good QoS (Quality of Service),the routing protocols must possess more data delivery ratio, less latency and less energy consumption.

Routing protocols can also be classified based on whether they are reactive or proactive. A proactive protocol sets up routing paths and states before there is a demand for routing traffic. Paths are maintained even there is no traffic flow at that time. In reactive routing protocol, routing actions are triggered when there is data to be sent and disseminated to other nodes. Here paths are setup on demand when queries are initiated. Routing protocols are also classified based on whether they are destination-initiated (Dst-initiated) or source-initiated (Src-initiated). A source-initiated protocol sets up the routing paths upon the demand of the source node, and starting from the source node. Here source advertises the data when available and initiates the data delivery. A destination initiated protocol, on the other hand, initiates path setup from a destination node. Routing protocols are also classified based sensor network architecture some WSNs consist of homogenous nodes, whereas some consist of heterogeneous nodes. Based on this concept we can classify the protocols whether they are operating on a flat topology or on a hierarchical topology. In Flat routing protocols all nodes in the network are treated equally. When node needs to send data, it may find a route consisting of several hops to the sink. A hierarchical routing protocol is a natural approach to take for heterogeneous networks where some of the nodes are more powerful than the other ones. The hierarchy does not always depend on the power of nodes. In Hierarchical (Clustering) protocols different nodes are grouped to form clusters and data from nodes belonging to a single cluster can be combined (aggregated).The clustering protocols have several advantages like scalable, energy efficient in finding routes and easy to manage.

10.3 Design Issues Of Routing Protocols

Initially WSNs was mainly motivated by military applications. Later on the civilian application domain of wireless sensor networks have been considered, such as environmental and species monitoring, production and healthcare, smart home etc. These WSNs may consist of heterogeneous and mobile sensor nodes, the network topology may be as simple as a star topology; the scale and density of a

network varies depending on the application. To meet this general trend towards diversification, the following important design issues of the sensor network have to be considered.

10.3.1) Fault Tolerance

Some sensor nodes may fail or be blocked due to lack of power, have physical damage or environmental interference. The failure of sensor nodes should not affect the overall task of the sensor network. This is the reliability or fault tolerance issue. Fault tolerance is the ability to sustain sensor network functionalities without any interruption due to sensor node failures.

10.3.2) Scalability

The number of sensor nodes deployed in the sensing area may be in the order of hundreds, thousands or more and routing schemes must be scalable enough to respond to events.

10.3.3) Production Costs

Since the sensor networks consist of a large number of sensor nodes, the cost of a single node is very important to justify the overall cost of the networks and hence the cost of each sensor node has to be kept low.

10.3.4) Operating Environment

We can set up sensor network in the interior of large machinery, at the bottom of an ocean, in a biologically or chemically contaminated field, in a battle field beyond the enemy lines, in a home or a large building, in a large warehouse, attached to animals, attached to fast moving vehicles, in forest area for habitat monitoring etc.

10.3.5) Power Consumption

Since the transmission power of a wireless radio is proportional to distance squared or even higher order in the presence of obstacles, multi-hop routing will consume less energy than direct communication. However, multi-hop routing introduces significant overhead for topology management and medium access control. Direct routing would perform well enough if all the nodes were very close to the sink. Sensor nodes are equipped with limited power source (<0.5 Ah 1.2V).Node lifetime is strongly dependent on its battery lifetime.

10.3.6) Data Delivery Models

Data delivery models determine when the data collected by the node has to be delivered. Depending on the application of the sensor network, the data delivery model to the sink can be Continuous, Event driven, Query-driven and Hybrid . In the continuous delivery model, each sensor sends data periodically. In event-driven models, the transmission of data is triggered when an event occurs. In query driven models, the transmission of data is triggered when query is generated by the sink. Some networks apply a hybrid model using a combination of continuous, event-driven and query driven data delivery.

10.3.7) Data Aggregation/Fusion

Since sensor nodes might generate significant redundant data, similar packets from multiple nodes can be aggregated so that the number of transmissions would be reduced. Data aggregation is the combination of data from different sources by using functions such as suppression (eliminating duplicates), min, max and average. As computation would be less energy consuming than communication, substantial energy savings can be obtained through data aggregation. This technique has been used to achieve energy efficiency and traffic optimization in a number of routing protocols

10.3.8) Quality Of Service (QoS)

The quality of service means the quality service required by the application, it could be the length of life time, the data reliable, energy efficiency, and location-awareness, collaborative-processing. These factors will affect the selection of routing protocols for a particular application. In some applications (e.g. some military applications) the data should be delivered within a certain period of time from the moment it is sensed.

10.3.9) Data Latency And Overhead

These are considered as the important factors that influence routing protocol design. Data aggregation and multi-hop relays cause data latency. In addition, some routing protocols create excessive overheads to implement their algorithms, which are not suitable for serious energy constrained networks.

10.3.10) Node Deployment

Node deployment is application dependent and affects the performance of the routing protocol. The deployment is either deterministic or self-organizing. In deterministic situations, the sensors are manually placed and data is routed through pre-determined paths. However in self organizing systems, the sensor nodes are scattered randomly creating an infrastructure in an Ad-hoc manner.

11. SECURITY IN WSN

A distributed Wireless Sensor Network (WSN) is a collection of n sensors with limited hardware resources. Sensors can exchange messages via Radio Frequency (RF), whose range usually covers only a limited number of other sensors. An interesting problem is how to implement secure pair-wise communications among any pair of sensors in a WSN. A WSN requires completely distributed solutions which are particularly challenging due to the limited resources and the size of the network.

Moreover, WSNs can be subject to several security threats, including the physical compromising of a sensor. Hence, any solution for secure pair wise communications should tolerate the collusion of a set of corrupted sensors. a probabilistic model and two protocols to establish a secure pair-wise communication channel between any pair of sensors in the WSN, by assigning a small set of random keys to each sensor. We build, based on the first Direct Protocol, a second Co-operative Protocol. The Co-operative Protocol is adaptive: its security properties can be dynamically changed during the life-time of the WSN. Both protocols also guarantee implicit and probabilistic mutual authentication without any additional overhead and without the presence of a base station. The performance of the Direct Protocol is analytically characterized while, for the Co-operative Protocol, we provide both analytical evaluations and extensive simulations. For example, the results show that, assuming each sensor stores 120 keys, in a WSN composed of 1024 sensors with 32 corrupted sensors the probability of a channel corruption is negligible in the case of the Co-operative Protocol. A Wireless Sensors Network (WSN) is a collection of sensors whose size can range from a few hundred to a few hundred thousands and possibly more sensors. The sensors do not rely on any pre-deployed network architecture, they thus communicate via an ad-hoc wireless network. Distributed in irregular patterns across remote and often hostile environments, sensors should autonomously aggregate into collaborative, peer-to-peer networks. Sensor networks must be robust and survivable despite individual sensor failures and intermittent connectivity (due, for instance, to a noisy channel or a shadow zone). WSNs are often infrastructure-less, and the power supply of each individual sensor is provided by a battery, whose consumption for both communication and computation activities must be optimized. A WSN can be deployed in both military and civil scenarios. For instance, it could be used to provide a relay network for tactical communication in a battlefield, collect data from a field in order to reveal the presence of a toxic gas, facilitate rescue operations in wide open hostile areas, fulfill perimeter surveillance duties, operate for commercial purpose in severe environmental constrained scenarios (for instance, to measure the concentration of metals such as nodules of manganese on the ocean bed). Moreover, a WSN can be used to enforce physical access control by checking secure access to a building. Each person should carry a sensor which contains some sort of encrypted personal information. This information is exchanged with other sensors distributed across the building, and can be used to authenticate, to assign the appropriate clearance to the users, and to trace their movements in the building. Establishing secure pair-wise communication can be useful for many applications. In particular, this is a pre-requisite for the implementation of secure routing. Also, it can be useful for the establishment of secure group communications as well. The native technique for implementing secure pair-wise communication is to assign a set of secret keys to each component of the group, each key of the set being shared with only one other member of the group. This solution requires each member to store n-1keys, where n is the size of the group, with n(n-1)/2 different keys in the group. We focus on confidentiality, and provide models and protocols to allow any pair of sensors of the WSN to establish a confidentially secure communication channel (secure channel in the following) while loading each sensor with a small set of keys. We devise a first protocol, the Direct Protocol, which establishes a pair-wise communication channel that is secure with a fixed probability. We then build on this protocol a second one that allows to trade off the desired level of security with the protocol overhead. The Co-operative Protocol is adaptive: its security parameters can be dynamically changed in such a way to guarantee a fixed security level even when the number of corrupted sensors in the WSN grows during the WSN life-time. We achieve this goal at the price of an increase in the communication overhead. Note that the overhead for establishing the communication channel is paid only once for any channel set up. The security of both approaches is analytically described, and these results have been validated with extensive simulations. We also show that both protocols guarantees implicit and probabilistic mutual sensor to sensor authentication with scaling properties.

12. METHODS PROVIDING SECURITY

Several recent research works focus on key establishment protocols_in dynamic peer groups. In particular, deals with the problem of key agreement in dynamic peer groups and recognizes that key agreement, especially in a group setting, is the stepping stone for_all the other security services. The paper also presents a concrete__protocol suite, CLIQUES, which offers complete key agreement services. CLIQUES is based on multi-party extensions of the well known Diffie-Hellman key exchange method. The protocols are provably secure against passive adversaries. In the above_protocols are enhanced to provide services like authenticated key agreement in dynamic peer groups with the emphasis on efficient__and provably secure key authentication, key confirmation and integrity. However, the protocols in and use public key cryptography._As it was pointed out in public key cryptography_is not well-suited for securing WSNs. Indeed, the memory of a__sensor is typically insufficient to hold the long keys necessary to guarantee secure asymmetric cryptographic. Moreover, sensors are_usually equipped with a low power processor which requires too long and too

much energy to compute the modular exponentiations involved in the implementation of public key cryptography. Among research specifically focused on a security subsystem for a limited wireless sensor network platform. The system assumes the presence of base stationsacting as gateways for inter-sensor communications. Being abase station more powerful (we can think of it as a workstation), it is reasonable to assume it can easily implement public key cryptography. By assuming the base stations trusted computing bases, can relax the assumption of tamper-resistance of sensors. The security subsystem is shown to support a few security functions, such as authenticated and confidentiality communications as well as authenticated broadcast. In, a key management scheme is proposed which periodically updates the symmetric keys employed by the sensors. However, neither forward nor backward secrecy is guaranteed. Different schemes for key establishment in WSN are examined and a couple of new schemes are proposed.

13 THREAT MODEL IN WSNS

Generally two types of attacks: (1) passive attacks; (2) active attacks. In passive attacks, we assume that an eavesdropper can constantly monitor the whole WSN. We consider two types of passive attacks that an adversary can perform: (1) cipher text attack, that is, given the cipher text, the adversary tries to recover the encryption key; and (2) chosen plain text attack, that is, the adversary can feed the sensor with known data and then observe the encrypted message sent by the sensor. Therefore, we consider confidentiality and authenticity of data of paramount importance. In active attacks, we assume the attacker can capture a sensor, collecting all the information and the keys the sensor is loaded with. Moreover, we consider a worst case scenario, that is we assume that all the compromised sensors in the WSN are compromised by the same attacker and thus collude to compromise the network. Finally, we assume that the environment in which the sensors operate is untrusted. Each sensor trusts itself, while sensors do not trust each other. To overcome these different protocols are introduced.

14. DIRECT PROTOCOL

The constraints that make the task of securing a channel between any pair of sensors not trivial include: a limited amount of memory and a limited battery power available to each sensor. Henceforth, we want to design a protocol that is,

- Memory efficient: only a limited amount of memory is required to store crypto keys;
- Energy efficient: low computation and communication overhead;
- Resilient to the coalition of corrupted sensors. To match these requirements, we will provide a key deployment scheme describing how the sensors are loaded with the keys a key discovery procedure which enables an arbitrary pair of sensors to compute the set of keys they share a security adaptive channel establishment procedure, a mechanism to enable an arbitrary pair of sensors to agree on a common key to be used to secure the channel.

14.1. The Key Deployment Scheme

Assume an n sensor Wireless Sensor Network. The random key pre-deployment strategy proposed is composed of the following steps:

1. a pool of P random keys $\{v^1_P \ldots\ldots\ldots\ldots v^p_p\}$ is generated;
2. for each sensor a in the WSN, a set $va=\{v^1_a \ldots\ldots\ldots v^k_a\}$. of k distinct keys is randomly drawn from the pool and assigned to a.

If the above key deployment scheme is used, the corresponding channel establishment procedure could be quite time and energy consuming. Even if two sensors a and b are in their communication range and share some keys, to discover which keys they actually share is not efficient. Indeed, sensor a is supposed to broadcast messages ,$E_{V^i_a}(\alpha)$, i = 1; : : : ;k where αis a challenge. The decryption of $E_{V^i_a}(\alpha)$ with the proper key by sensor b would reveal the challenge and the information that b shares that key with a. This key discovery procedure requires k2 decryptions on the receiver side and k encryptions on the sender side. Moreover, at least k messages have to be sent and received.

As observed in, a pseudo-random key deployment scheme allows a more efficient key discovery procedure than a random scheme. Given a sensor a, the idea is to generate the indexes of the keys that will be assigned to a pseudo-randomly. The generator is initialized with a publicly known seed dependent on a. Once the seed is known, the k indexes of the keys assigned to a can be computed by anyone. Note that this key discovery procedure reveals only the indexes of the keys given to sensor a, and does not leak any information on the keys themselves. The above pseudo-random method requires a limited amount of additional storage per sensor in comparison with the key assignment. Indeed, each sensor has to store, along with the keys, also the index of each key. However, the new key discovery procedure now requires no message exchange, at most k applications of the pseudo-random generator, and k look-ups in the local memory.

In the following we adopt this pseudo-random, seed-based key deployment strategy, and for this strategy we are interested in evaluating its main properties: (1) the channel establishment effectiveness between any two sensors; (2) the efficiency of the channel establishment procedure; (3) the resilience of the channel against node

capture.

14.2. Channel Existence

Given two sensors a and b loaded with sets of keys Va and Vb according to the seed-based strategy, it is important to assess the probability that a channel exists between two sensors in the WSN.

A communication channel (channel in the following) exists between sensors a and b if and only if Va \Vb =6 that is a and b share at least one key.

From Definition, the probability that a channel exists between sensors a and b is equal to the probability that a and b share at least one key of the pool. Let E be the event: "There is at least one key shared by a and b". $\mathbf{P_r}[E]$ can be directly computed as

Cooperative protocol.

$$\mathbf{Pr}[E] = 1 - \mathbf{Pr}[\overline{E}] = 1 - \frac{\binom{P-k}{k}}{\binom{P}{k}}.$$

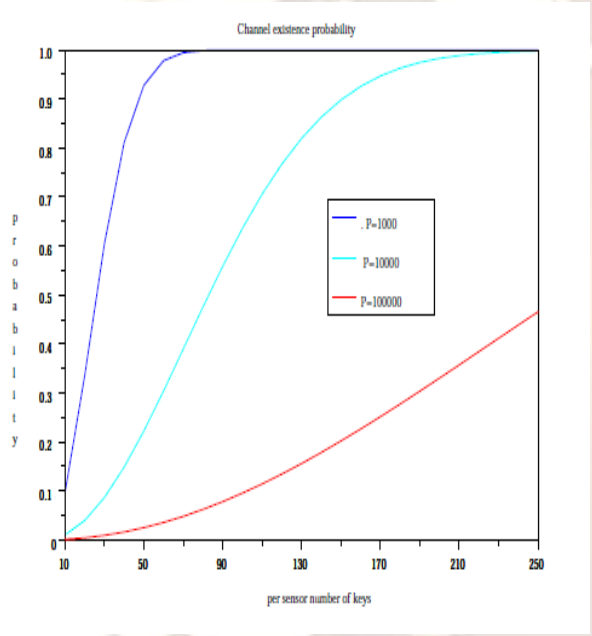

Fig 2: Channel existence probability for different values of P and k.

Note that channel existence scales with the WSN size. Indeed, the probability of channel existence is independent from n, being dependent only on k and P. In Fig 2 we plot the probability of channel existence between sensors a and b as a function of the per sensor number of keys k and for three values of the pool size P. It is remarkable that, even with a small number of keys loaded on the sensors, the channel has high probability of existence.

15. THE COOPERATIVE PROTOCOL

15.1. The Protocol

As it has been shown the Direct Protocol allows two sensors to communicate with a certain degree of security. The degree of security achieved depends on parameters k, P according to methodology. The main drawbacks of the Direct Protocol are the following the Direct Protocol is not adaptive to changes in the threat (for instance, the number of corrupted sensors overcomes the value assumed as an upper bound in the design project of the WSN), or in the security requirements (for instance, a higher security level is desired due to the temporary management of more sensitive information), for a fixed sensor key ring size k, the probability of channel corruption can be unsatisfactory even for small values of the number of corrupted sensors

TABLE 2

Pseudo code of the Co-operative Protocol for the pair wise key establishment

Co-operative_Protocol(b :sensor)
Input: the receiving sensor;
Output: $k_{a,b}^{\mathcal{C}}$ and the set of co-operating sensors $\mathcal{C}$

1. Generate set $\mathcal{C}$;
2. Set time-out Δ;
3. $k_{a,b}^{\mathcal{C}} = 0$;
4. **for all** $c \in \mathcal{C}$ **do begin**
5. $k_{a,c} = \text{Direct\_Protocol}(c)$;
6. $a \rightarrow c :< a, c, E_{k_{a,c}}(\text{req\_key} || b) >$
7. **end**;
8. $\mathcal{C}' = \mathcal{C}$;
9. **while** ($\mathcal{C}' \neq \emptyset$ **and** (**not** elapsed(Δ))) **do begin**
10. $a \leftarrow c :< c, a, E_{k_{c,a}}(HMAC(ID_a, k_{c,b})) >$;
11. $s = E_{k_{a,c}}^{-1}(E_{k_{a,c}}(HMAC(ID_a, k_{c,b})))$;
12. $\mathcal{C}' = \mathcal{C}' - \{c\}$;
13. $k_{a,b}^{\mathcal{C}} = k_{a,b}^{\mathcal{C}} \oplus s$
14. **end**
15. $k_{a,b}^{\mathcal{C}} = k_{a,b} \oplus k_{a,b}^{\mathcal{C}}$;
16. $a \rightarrow b :< a, b, E_{k_{a,b}}(\mathcal{C}) || \mathcal{H}(k_{a,b}^{\mathcal{C}}) >$;

assuming 16 corrupted sensor, the best (lowest) channel corruption probability is reached around k = 100 and is above 15%).

To overcome the above drawbacks, we propose a scheme where, with an increase in the communication overhead, the key establishment phase is made co-operative. If sensor a wants to establish a secure channel with sensor b, sensor a chooses a set C = $\{c_1; : : : ;c_m\}$ of co-operating sensors such that a;b € C and m ≥ 0. Then, a sends a request of co-operation to each of the sensors in C. The request sent to c ε C is encrypted with $k_{a,c}$ and carries the ID of b. Each cooperating sensor c transforms its original channel key with b, kc;b, as follows: first, kc;b is built according to the Direct Protocol; then, a share is created by hashing kc;b with the id of a

$$HMAC(ID_a, k_{c,b});$$

finally, the share is sent back to a encrypted with key $k_{a;c}$. When all the shares are received, sensor a computes $k_{a;b}$ and combines it with all the shares to obtain a cooperative channel key $k^C_{a;b}$

$$k^C_{a,b} = k_{a,b} \oplus \left(\bigoplus_{c \in C} HMAC(ID_a, k_{c,b}) \right).$$

Sensor a sends the list of sensors in C (encrypted with key ka;b) to sensor b along with H (kC a;b). Sensor b, once this message is received, has all the information required to locally compute kC a;b, without sending or receiving any other message, and to double check the resulting key with H (kC a;b). Note that, when m = 0, the Direct and Co-operative Protocol are equivalent.

Table 3 shows in detail the pseudo code of the Co-operative Protocol. In Figure 3, we show a simplified instance of the messages exchanged by the Co-operative Protocol in the case there is only one co-operating sensor (c1). In step (1), sensor a sends the request of co-operation to sensor c1; once c1 has received such a request, it computes kc1;b according to the Direct Protocol and sends a transformed and not-invertible image of such a value to a, as shown in step (2). Finally, sensor a computes k^Ca;b according to Equation, and sends this value to b, together with the set of sensors (c1) that co-operated in building the channel (step (3)). Note that it is mandatory for sensor a to send, in step (3), the list of sensors in C, otherwise b would not be able to compute k^Ca;b. Such a list is at most mlogn bits long.

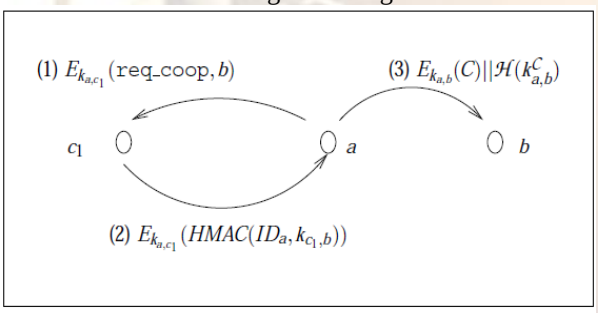

Fig 3: Example of co-operative approach with one cooperating sensor

Set C can be chosen according to several policies. A first energy preserving option is to include only relatively nearby sensors in C. For example, only sensors within one or two hops. This choice yields a more efficient key setup phase, though the protocol can be weaker against geographically localized attacks. A second option is to choose C randomly, giving more security at the price of a larger communication overhead especially in large networks. With this second option, the protocol would support both random and geographically localized attacks. Third, sensors can be chosen according to individual properties, like tamper-resistance, giving a potentially more secure channel.

The Co-operative Protocol shows the following features:

- sensor failure resistance: if a sensor in C is not available for any reason (for instance, the sensor is destroyed or its battery exhausted), the protocol will not fail or deadlock; moreover, if some sensors do not answer to the request of co-operation within a certain time-out, sensor a can choose to add other sensors to C, in order to achieve a satisfactory level of security.
- no information leakage: since co-operating sensors provide a with a transformed, not-invertible image of their channel with b, no information on the effective channels $k_{ci;b}$ is revealed;
- adaptiveness: if no information is available on the set of corrupted sensors but an upper bound on set C can be chosen in such a way to secure all channels with the desired probability;
- load balance: the work-load generated by the Co-operating Protocol is equally distributed among all the sensors in C, i.e. one message per sensor in C. Only sensor a has to send m+1 messages (one for each of the co-operating sensors in C and one to b). The total cost for the WSN is thus 2_{m+1} potentially multi-hop messages. However, this cost is incurred only once, during the channel set up. Finally, note that sensor b does not need to send any message to build up the cooperative channel.

In general, it is possible that corrupted sensors are chosen as co-operators in the Co-operative Protocol. This is explicitly considered in the analysis of the previous section and in the experiments, which shows that channel confidentiality can be probabilistically guaranteed. However, it is interesting to explore all possible attacks from a cooperating sensor against other properties of the protocol. Assume ὼi 2 C \W is a corrupted sensor included into the set of cooperators for the channel set up from a to b. When ὼi is asked by a to provide its share, i can behave as follows:

1. Sensor $\grave{\omega}_i$ does not respond;
2. sensor $\grave{\omega}_i$ sends a correct key $k\grave{\omega}_{i;b}$;
3. sensor $\grave{\omega}_i$ sends a bogus key $\tilde{k}\grave{\omega}_{i;b}$.

Case 1 is equivalent to the case when a co-operating sensor is not available anymore, for instance it has been destroyed or its battery has run out. After the time-out Δdefined in Table 3, sensor a can decide to involve other sensors if the number of cooperating sensors is too low to guarantee its security requirements. Case 2 is the best choice if the attacker aims at breaking the channel confidentiality. Indeed, the channel is set up, and the attacker may have enough keys to recover k^Ca;b. Since this paper focuses on confidentiality, in both the analysis and the experimental evaluation we assume this is the default behavior of corrupted sensors. Note that the presence of malicious cooperators does not imply that

the channel is corrupted. Case 3 may result in a Denial of Service (DoS) on sensor a. Indeed, the channel built by sensor a with a bogus share does not match the channel locally computed by sensor b. Even though the goal of this paper is to address confidentiality, in the following we sketch a few countermeasures that can be taken to mitigate this sort of DoS attack. A first countermeasure is to randomly select another set C of co-operating sensors and to re-apply the co-operative protocol. In order to be an effective solution, set C should be chosen small enough to have Pr[C ∩W = ϕ] > 1=t, for some small positive integer t. In this way, after t iterations on the average, a good set of cooperators is found. Note that other subsets of cooperators can be added later to strengthen the same final cooperative channel. A second countermeasure is possible if a trusted channel to the center is available. Each sensor can store an individual secret key shared with the center, which also knows all the secret keys of the pool. When sensor a finds that a channel key ˜k Ca ;b could contain a bogus share, sensor a sends it to the center along with all the shares it used to build the key. Assuming that a is not corrupted, the center has all the information to track down efficiently the cheating sensors among C and b. Then, this is sent back to a. Note that the center is used only when a cheater is detected, and corrupted sensors are discouraged to give bogus shares in this setting. Finally, even when a channel to the center is not available, the presence of a bogus share gives the important information that the WSN is under attack.

CONCLUSION

Sensor Networks hold a lot of promise in applications where gathering sensing information in remote locations is required. It is an evolving field, which offers scope for a lot of research. Moreover, unlike MANETS, sensor networks are designed, in general, for specific applications. Hence, designing efficient routing protocols for sensor networks that suits sensor networks serving various applications is important. In this paper, we identified some of the important design issues of routing protocols for sensor networks and also compared and contrasted the existing routing protocols. As our study reveals, it is not possible to design a routing algorithm which will have good performance under all scenarios and for all applications. Although many routing protocols have been proposed for sensor networks, many issues still remain to be addressed Other possible future research for routing protocols includes the integration of sensor networks with wired networks (i.e. Internet). Most of the applications in security and environmental monitoring require the data collected from the sensor nodes to be transmitted to a server so that further analysis can be done. On the other hand, the requests from the user should be made to the sink through Internet. Since the routing requirements of each environment are different, further research is necessary for handling these kinds of situations.

The primary contribution of this work is to provide an brief analytic and quick review about sensor networks, wireless sensor networks, routing protocols, design issues, and security constraints by going through this paper an easier and brief review of all wsns and the drawbacks of protocols which using for providing security has also analyzed and the disadvantages are also mentioned… to continue forwarding the field of security in WSN reprogramming protocols, proposing a comprehensive security solution. We focus less on novel solutions for authentication and focus more on availability and confidentiality .in network scenarios needing security in the reprogramming process. Another contribution of this work is that we make evident in our energy examination that radio operations are the most energy consuming operations in update dissemination. This fact guided our decisions in proposing balanced availability and confidentiality solutions.

REFERENCES

[1] A comparative analysis of routing techniques for wireless sensor networks Raghunandan, G.H. Lakshmi, B.N. Innovations in Emerging Technology (NCOIET), 2011 National Conference on Digital Object Identifier: 10.1109/NCOIET.2011

[2] The Novel Energy Adaptive Protocol for heterogeneous wireless sensor networks Golsorkhtabar, M.; Nia, F.K.; Hosseinzadeh, M.; Vejdanparast, Y. Computer Science and Information Technology (ICCSIT), 2010 3rd IEEE International Conference on Volume: 2
Digital Object Identifier: 10.1109/ICCSIT.2010.5563781 Publication Year: 2010 , Page(s): 178 - 182

[3] Tradeoffs among Delay, Energy and Accuracy of Partial Data Aggregation in Wireless Sensor Networks Wuyungerile Li; Bandai, M.; Watanabe, T. Advanced Information Networking and Applications (AINA), 2010 24th IEEE International Conference on Digital Object Identifier: 10.1109/AINA.2010.137 Publication Year: 2010 , Page(s): 917 – 924

[4] Methods of Sensors Localization in Wireless Sensor Networks Chaczko, Zenon; Klempous, Ryszard; Nikodem, Jan; Nikodem, Michal Engineering of Computer-Based Systems, 2007. ECBS '07. 14th Annual IEEE International Conference and Workshops on the Digital Object Identifier: 10.1109/ECBS.2007.48

[5] A reliable synchronous transport protocol for wireless image sensor networks

Boukerche, A.; Yan Du; Jing Feng; Pazzi, R. Computers and Communications, 2008. ISCC 2008. IEEE Symposium on Digital Object Identifier: 10.1109/ISCC.2008.4625679 Publication Year: 2008 , Page(s): 1083 - 1089

[6] An implementation of wireless sensor network Soo-Hwan Choi; Byung-Kug Kim; Jinwoo Park; Chul-Hee Kang; Doo-Seop Eom Consumer Electronics, IEEE Transactions on Volume: 50 , Issue: 1 Digital Object Identifier: 10.1109/TCE.2004.1277868 Publication Year: 2004 , Page(s): 236 - 244

[7] W. Heinzelman, J. Kulik, H. Balakrishnan, Adaptive protocols for information dissemination in wireless sensor networks, in: Proceedings of the 5th Annual ACM/IEEE International Conference on Mobile Computing and Networking

[8] Ian F. Akyildiz, Weilian Su, Yogesh Sankaraubramaniam, and Erdal Cayirci: A Survey on sensor networks, IEEE Communications Magazine (2000)

[9] Al-Karaki,J.N,Al-Mashagbeh: Energy-Centric Routing in Wireless Sensor Networks Computers and Communications, ISCC 06 Proceedings, 11th IEEE Symposium (2002).

[10] Kay Romer, Friedemann Mattern: The Design Space of Wireless Sensor Networks, IEEE Wireless Communications, pp. 54-61 (December 2005)

AUTHORS BIBILOGRAPHY

M.L.S.N.S Lakshmi received her diploma in Electronics and Communications in Govt. Polytechnic for Women Guntur (Andhra Pradesh) in (2008),B.Tech degree in Electronics And Communication Engineering from Vignan's Engineering college affiliated to JNTU Kakinada, (in 2011) and presently doing her M.Tech in Communications and Radars from Koneru Lakshmaiah University (KLU) situated in Vaddeswaram near to Vijayawada (Andhra Pradesh). Currently she is doing research at the laboratories of mobile and wireless communications in the Department of Electronics and Communication Engineering at KL University. Her research interests lie in channel allocation strategies, assignment schemes, hand off techniques, call blocking probabilities, access& queuing techniques, related to mobile and wireless communications.

Gopi Krishna.Seemala received B.S.C electronics degree from Andhra university Visakhapatnam (Andhra pradesh) in 1999.and M.S.C electronics in 2001,and doctorate in physics(phd)from same university in 2002.from 2002-2007 he worked as a senior research fellow in Andhra University under the Guidance of PROF.P.V.S RAMA RAO Physics Dept, Andhra University and from 2007 he worked as a research scientist in Institute For scientific research ,Boston college, Boston U.S.A. later he worked as a post doctoral research scientist (2007-2009) in the same college .having Hands on experience on Real time monitoring TEC, and scintillations using the LISN(low latitude ionospheric sensor network)producing TEC maps and possible prediction of scintillations. He published more than 20 research publications in terristial atmospheric, and oceanic sciences journal of geophysical research, Journal of earth planets and sciences, journal of atmospheric and solar terristial physics and presented papers on communication journals. Presently he is working as a associate professor in Koneru Lakshmaiah university.