International Journal of Computer Science and Engineering Communications,
Vol.5, Issue.1 (2017):Page.1502-1510
IJCSEC.COM

Intrinsic Secrecy in Wireless Sensor Network

E.S.Vijay Shankar[1], Venkatesan[2]
[1]*Research Scholar, St.Peter's University, Chennai.*
[2]*Asst.Prof. Dept. of Computer Applications, St.Peter's University, Chennai*
es.vijaysharmar@gmail.com

Abstract-
The ability to exchange secret information is critical to many commercial, governmental, and military networks. Wireless sensor intrinsic secrecy is essential for communication confidentiality, health privacy, public safety, information superiority, and economic advantage in the modern information society. Wireless Sensor security schemes have typically evolved from those developed for traditional wire line applications, these schemes do not consider physical properties of the wireless channels. To overcome these problems, this research work develops a foundation for design and analysis of wireless sensor networks with secrecy provided by intrinsic properties such as node spatial distribution, wireless propagation medium, and aggregate network interference.

1 INTRODUCTION

The field of sensor network is well known due to its popularity in research community. It is a collection of thousands of self-organized sensor nodes capable of wireless communication. Since the nodes are not so wealthy in terms of resources, therefore complex algorithms cannot be played over it. Security is the main preconcert to socialize this network for common usage. For making the WSN secure, cryptography plays an important role. There are many algorithms proposed so far: symmetric, asymmetric and hybrid. But complex algorithms, which had been proposed for MANETs, are not successful over WSN. To design the network cryptographically (completely) secure, security must be integrated into every node of the network. So security should be implemented at every point of the network. Cryptography is a standard method to provide security in a network. But here in WSN, cryptographic algorithms should be designed such that it is robust in nature but does not use more memory, more power, and more energy so as the lifetime of the is also dependent upon the nature of the application and algorithm might be specific to the application. Basically the major challenge for employing any efficient security scheme in wireless sensor networks is created by the size of sensors, consequently the processing power memory and type of tasks expected from the sensors To address the critical security issues in wireless sensor networks we talk about cryptography, steganography and other basics of network security and their applicability. We explore various types of threats and attacks against wireless sensor network in reviews the related works and proposed schemes concerning security in WSN and also introduce the view of holistic security in WSN. Finally concludes the paper delineating the research challenges and future trends toward the research in wireless sensor network security. Current WSN security solutions rely on secret keys but today an efficient key management protocol is still needed to generate, distribute, renew and revoke cryptographic keys.

1.1 Overview

In the last few years, several key management protocols for WSN have been denned, but they do not satisfy the protocol efficiency requirements as follows:

1. Low storage, computation, and transmission overheads.

2. Resistance to nodes compromising, so keys established between non compromised nodes remain confidential even in case of nodes compromising.

2. TYPES OF SENSOR NETWORKS

TERRESTRIAL WSNS

In these, nodes are distributed in a given area either in an ad hoc manner (sensor nodes are randomly placed into the target area by dropping it from plane) or in pre-planned manner (sensor nodes are placed according to grid placement, optimal placement, 2-d and 3-d placement models). Since battery power is limited and it cannot be recharged, terrestrial sensor nodes must be provided with an optional power source such as solar cells.

UNDERGROUND WSNS

In these, sensor nodes are buried underground or in a cave or mine that monitors the underground conditions. Sink nodes are deployed above the ground to forward the gathered information from the sensor nodes to the base station. These are more expensive than the terrestrial sensor networks because proper nodes are to be selected that can assure reliable communication through soil, rock, water and other mineral contents.

UNDERWATER WSNS

In these, sensor nodes and vehicles are located underwater. Autonomous vehicles are used for gathering the data from the sensor nodes. Sparse deployment of nodes is done in this network. Main problems that come under this while communicating are limited bandwidth, long propagation delay and signal fading issue.

MULTIMEDIA WSNS

In these, low cost sensor nodes are equipped with cameras and microphones. These nodes are located in a pre-planned manner to guarantee coverage. Issues in these networks are demand of high bandwidth, high energy consumption, quality of service provisioning, data processing and compression techniques, and cross layer design.

3. SECURITY REQUIREMENTS WSN CONFIDENTIALITY

Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. A loss of confidentiality is the unauthorized disclosure of information. In a WSN, the issue of confidentiality should address the following requirements:
(i) A sensor node should not allow its readings to be accessed by its neighbors unless they are authorized.
(ii) Key distribution mechanism should be extremely robust
(iii) Public information such as sensor identities, and public keys of the nodes should also be encrypted in certain cases to protect against traffic analysis attacks.

AUTHENTICATION

Authentication ensures the reliability of the message by identifying its origin. By authenticating other nodes, cluster heads, and base stations before granting a limited resource, or revealing information.

INTRINSIC

Intrinsic ensures the reliability of the data and refers to the ability to confirm that a message has not been tampered with, altered or changed while on the network.

In a WSN, the issue of integrity should address the following requirements:

(i) Only the nodes in the network should have access to the keys and only an assigned base station should have the privilege to change the keys. This would effectively thwart unauthorized nodes from obtaining knowledge about the keys used and preclude updates from external sources.

(ii) It protects against an active, intelligent attacker who might attempt to disguise his attack as noise.

AVAILABILITY

Availability ensuring timely and reliable access to and use of information. A loss of availability is the disruption of access to or use of information or an information system. In a WSN, the issue of availability should address the following requirements:

(i) The security mechanisms should be available all the time; a single point of failure should be avoided,

(ii) The mechanism is used as a central access control system to ensure successful delivery of every message to its recipient node.

DISTRIBUTED SENSOR NETWORK

If a centralized architecture is used in a sensor network and the central node fails, then the entire network will collapse, however the reliability of the sensor network can be increased by using a distributed control architecture. Distributed control is used in WSNs for the following reasons:

1. Sensor nodes are prone to failure,
2. For better collection of data,
3. To provide nodes with backup in case of failure of the central node.

There is also no centralized body to allocate the resources and they have to be self-organized.

DATA INTEGRATION AND SENSOR WEB

The data gathered from wireless sensor networks is usually saved in the form of numerical data in a central base station. Additionally, the Open Geospatial Consortium (OGC) is specifying standards for interoperability interfaces and metadata encodings that enable real time integration of heterogeneous sensor webs into the Internet, allowing any individual to monitor or control wireless sensor networks through a web browser.

4. NETWORK PROCESSING

To reduce communication costs some algorithms remove or reduce nodes' redundant sensor information and avoid forwarding data that is of no use. As nodes can inspect the data they forward, they can measure averages or directionality for example of readings from other nodes. For example, in sensing and monitoring applications, it is generally the case that neighboring sensor nodes monitoring an environmental feature typically register similar values. This kind of data redundancy due to the spatial correlation between sensor observations inspires techniques for in-network data aggregation and mining.

5. CURRENT RESEARCH AND DEVELOPMENT TRENDS

Applications and Deployment

Several applications have been benefited from the advances in wireless sensor networks. These include Agriculture, Health Care, Defense, Wild Life Habitat Monitoring, Under Water monitoring, Disaster Management (Safety) and Industrial (monitoring, control, factory automation) applications. For all these applications, research deployments have been conducted and products incorporating WSNs are appearing. The current research hence focuses on application-driven systems in order to address more concrete issues. Preliminary results obtained from these deployments are encouraging and widespread use is highly likely. WSNs are capable of enhancing system performance significantly so they hold considerable promise to Industry. WSN technology is slowly graduating from the researcher "market" to the early adopters in industry. Several start-up companies are offering products in the sensor networking domain: Sentilla, Sensicast, Point8, Arch Rock, Synapses, Crossbow, sensorial, and others. Industrial research labs have also funded sensor networking research. In some cases, the technology is showing up in vertical niche markets, e.g., in process control, where it is not even advertised as WSN. The military continues to fund research in this area, now more so in the context of aiding mobile dismounts/units, but is yet to seriously adopt the technology in its operation. A recent issue of IEEE Spectrum classified WSNs as one of the top 10 emerging technologies. Eventually, it is felt by most of the research community that it will pervade into daily life like the cell phone technology.WSNs may either connect to the rest of the world through the cellular network or through the wired internet. In any case WSN impact on the traditional networks is likely to be transformative, simply by taking into account the amount of data that will enter/leave as machines talk to enterprises and other machines. WSNs have a major role to play in cyber-physical systems, pervasive computing, Body Networks and Internet of Things. According to Fredonia Group report on sensors, 2002, Sensor market in 2001 was approximately $11 Billion while the Wiring installation costs were more than $100 Billion. With recent advances and availability of wireless sensor device that can be battery powered the cost of wiring would be the major saving. Further over-the-air programming and solar power sensor devices, helps in reducing the deployment and maintenance cost to a large extent. Activities Spurred due to WSNs WSN research has spurred

Activity on Several Fronts

i. Ad hoc networks
ii. Distributed computing
iii. Decision making.
iv. This helps in more on device computation in order to reduce network traffic/communication and hence increase network life.
v. Low power electronics/low power modem design. The current status of WSN technology includes algorithm design as well as hardware design. However, the real challenge is deploying long-lasting systems in the real environments given the issues such as energy efficiency, self-configuration (low management cost) and low cost hardware design.

Contrasting Views

Interest in WSNs across industry and academia continues to be very high, although we are now experiencing a bit of a "backlash" due to the large number of academic research groups getting involved and few successes commercially to date. The vast popularity of WSNs as a research field for academia has left some to feel that it is becoming difficult to make fundamental contributions although the field is still very young. There is also a sense of ossification behind the TinyOS and mote platforms which are premature since many application domains involve quite different hardware and software demands than provided by that system. This “second system effect” will likely subside over the next year or so and it will become clearer where the lasting contributions and research directions lie.

Research Issues

Some of the research issues are:

i. Transducer design: Developing new sensor transducers that are compact, low power, and cost effective. Bio-degradable / environment-friendly sensor design.
ii. Electronic system design: The system design is one of the promising challenge areas where several new breakthroughs are possible in the near term leading to fundamentally new design directions. Integrating sensors with the appropriate electronic circuitry to extract digital data, using sensor feedback to enhance the data collection within the electronics, and providing low noise outputs using sensor arrays.
iii. Node design: Developing low power sensor nodes with appropriate processing and networking capabilities.
iv. System Design: Developing sensor networks of several nodes and integrating them with application specific information systems.
v. Protocol: Distributed algorithms, Power Aware Routing, Dissemination, Time Synchronization, Security, Middleware, Localization of sensors, Data aggregation Techniques, Multimodal sensor fusion, Energy-Efficient realtime Scheduling. In the following section we briefly review research in detection and tracking using WSNs.

APPLICATIONS OF WSN AND INTRINSIC SECRECY

To demonstrate the capabilities of wireless sensor networks we present two examples of applications and associated systems for those applications.

SURVEILLANCE AND TRACKING

The Vigil Net system is a long-lived real-time wireless sensor network for military surveillance. The general objective of VigilNet is to alert military command and control units of the occurrence of events of interest in hostile regions. The events of interest are the presence of people, people with weapons, and large and small vehicles. Successful detection, tracking and classification require that the application obtain the cur-rent position of an object with acceptable precision and confidence. When the information is obtained, it is reported to a remote base station within an acceptable latency. Vigil Net is an operational self-organizing sensor network (of over 200 XSM mote nodes) to provide tripwire-based surveillance with a sentry-based power management scheme, in order to achieve minimum 3 to 6 months lifetime. The tripwire also activates additional external (i.e., out of the Vigil net system proper) sensors, e.g., infrared cameras, only when necessary, thereby also increasing their lifetimes as well provides an overview of the Vigil Net architecture, in which there are three categories of

6. COMPONENTS

1) Application components.
2) Middleware components.

3) TinyOS system components.

The application components are specially designed for surveillance purposes. It includes
1) An entity-based tracking service.
2) Classification components,
3) Which provide four types of target dierentiation,
a. Velocity calculation.
b. Which providestarget speed and bearing estimation.
c. False alarm filtering.
d. Which dierentiates between real and false targets.

Middleware components are designed to be application independent. Time synchronization, localization, and routing comprise the lower-level components and form the basis for implementing the higher-level middleware services, such as aggregation and power management. Time synchronization and localization are important for a surveillance application because the collaborative detection and tracking process relies on the spatiotemporal correlation between the tracking reports sent by multiple motes. The time synchronization module is responsible for synchronizing the local clocks of the motes with the clock of the base station. The localization module is responsible for ensuring that each mote is aware of its location. The configuration module is responsible for dynamically reconfiguring the system when system requirements change. Asymmetric detection is designed to aid the routing module to select high-quality communication links. The radio wakeup module is used to alert non-sentry motes when significant events happen. Power management and collaborative detection are two key higher-level services provided by Vigil Net. The sentry service and tripwire management are responsible for power management, while the group management component is responsible for collaborative detection and tracking of events. The sentry and tripwire services conserve energy of the sensor network by selecting a subset of motes, which are defined as sentries, to monitor events. The remaining motes are allowed to remain in a low-power state until an event occurs. When an event occurs, the sentries awaken the other motes in the region of the event and the group management component dynamically organizes the motes into groups in order to collaboratively track. Together, these two components are responsible for energyecient event tracking. The Vigil Net architecture was built on top of TinyOS. .

These components provide low-level support for Vigil Net modules, which are also written in Nest C. Components from TinyOS and VigilNetapplications are processed by the NesC compiler into a running executable, which runs (in the Vigil Net case) on the XSM (and MICA2) mote platforms.AlarmNet a medical-oriented sensor network system for large-scale assisted living facilities, integrates heterogeneous devices, some wearable on the patient and some placed inside the living space. Together they inform the healthcare provider about the health status of the resident. Data is collected, aggregated, pre-processed, stored, and acted upon using a variety of replaceable sensors and devices (activity sensors, physiological sensors, environmental sensors, pressure sensors, RFID tags, pollution sensors, floor sensors, etc.). Multiple body networks are present in the system. Traditional healthcare provider networks may connect to the system by a residential gateway, or directly to their distributed databases. Some elements of the network are mobile such as the body networks as well as some of the infrastructure network nodes, while others are stationary. Some nodes can use line power, but others depend on batteries. The system is designed to exist across a large number of living units. The system architecture for Alarm Net is shown in Figure. Each tier of the architecture is briefly described below.

Body Networks and Front-ends. The body network is composed of tiny portable devices equipped with a variety of sensors (such as heart-rate, heart-rhythm, temperature, pulse oximeter, accelerometer), and performs biophysical monitoring, patient identification, location detection, and other desired tasks. Their energy consumption is also optimized so that the battery is not required to be changed regularly. They may use kinetic recharging. Actuators notify the wearer of important messages from an external entity. For example, an actuator can remind an early Alzheimer patient to check the oven because sensors detect an abnormally high temperature. Or, a tone may indicate that it is time to take medication. A node in the body network is designated as the gateway to the emplaced sensor network.

Due to size and energy constraints, nodes in this network have little processing and storage capabilities.

i. Emplaced Sensor Network. This network includes sensor devices deployed in the assisted living environment (rooms, hallways, units, furniture) to support sensing and monitoring, including: motion, video cameras, temperature, humidity, acoustic, smoke, dust, pollen, and gas.

ii. All devices are connected to a more resourceful backbone. Sensors communicate wirelessly using multi-hop routing and may use either wired or battery power. Nodes in this network may be physically moved and may vary in their capabilities.

iii. Backbone. A backbone network connects traditional systems, such as PDAs, PCs, and in-network databases, to the emplaced sensor network. It also connects sensor nodes by a high-speed relay for ancient routing. The backbone may communicate wirelessly or may overlay onto an existing wired infrastructure. Some nodes possess significant storage and computation capability, for query processing and location services. Yet, their number, depending on the topology of the building, is minimized to reduce cost.

iv. In-network and Back-end Databases. One or more nodes connected to the backbone are dedicated in-network databases for real-time processing and temporary caching. If necessary, nodes on the backbone may serve as in-network databases themselves. Back-end databases are located at the medical center for long-term archiving, monitoring and data mining for longitudinal studies.

HUMAN INTERFACES.

Patients and caregivers interface with the network using PDAs, PCs, or wearable devices. These are used for data management, querying, object location, memory aids, and configuration, depending on who is accessing the system and for what purpose. Limited interactions are supported with the on-body sensors and control aids. These may provide memory aids, alerts, and an emergency communication channel. PDAs and PCs provide richer interfaces to real-time and historical data. Caregivers use these to specify medical sensing tasks and to view important data. The software components of the Alarm Net architecture are shown in Figure 1.3. Sensor devices require components for sensing, networking, power management, handling queries and supporting security. The Stargates implement significantly more functionality including increased security, privacy, query management and database support. Here we briefly present the role played by wireless sensor network in applications ranging from environmental monitoring, industrial automation, agriculture, disaster control, automotive, structure health monitoring.

1. SECURITY AND SURVEILLANCE

Security and detection are the important applications of wireless sensor networks. Sensor nodes with motion sensing capabilities may be deployed at the borders to detect the intruder crossing the line of control. Hence surveillance of regions, assets, perimeters, borders and cleared areas can be efficiently done by deploying wireless sensor networks.

2. ENVIRONMENTAL

Monitoring Following are some of the projects and research plans sought in the environment monitoring application of wireless sensor networks.

i. **Watershed**

Correctly managing our watersheds is essential to ensure water supply to the increasing human population in the world. Collecting data for understanding the water systems of rivers and lakes including the impact of environmental factors and human activity.

ii. **Scientific investigation**

Sensor networks are being used for various scientific explorations including ecological and environmental ones.

iii. **Pollution monitoring**

Growing urban and industrial regions need efficient pollution monitoring technology.

7. CONCLUSION

The intrinsic secrecy in wireless sensor networks continues to grow and become widely used in many applications. So, the need for security becomes vital. However, the wireless sensor network suffers from many constraints such as limited energy, processing capability, and storage capacity, etc. Consequently, many innovative security protocols and techniques have been developed to meet this challenge. There are many ways to provide secrecy, one is cryptography. Selecting the most appropriate cryptography method for sensor nodes is fundamental to provide security provider intrinsic secrecy in WSNs.

REFERENCES

1. Prabal Dutta, Jay Taneja, Jaein Jeong, Xiaofan Jiang, and David Culler, "A Building Block Approach to Sensornet Systems", In Proceedings of the Sixth ACM Conference on Embedded Networked Sensor Systems (SenSys'08), Nov. 5-7, 2008. © ACM, 2008.
2. Sukun Kim , Shamim Pakzad , David Culler , James Demmel , Gregory Fenves , Steven Glaser , Martin Turon, “Health Monitoring of Civil Infrastructures Using Wireless Sensor Networks” In IPSN ’07: Proceedings of the 6th international conference on Information processing in sensor networks.
3. Shamim N. Pakzad, Gregory L. Fenves, Sukun Kim, and David E. Culler, “Design and Implementation of Scalable Wireless Sensor Network for Structural Monitoring”, In ASCE Journal of Infrastructure Engineering, March 2008, Volume 14, Issue 1, pp. 89-101.
4. Sazonov et. al., “Wireless Intelligent Sensor Network for Autonomous Structural Health Monitoring”, Proc. SPIE, Vol. 5384, 305 (2004); doi:10.1117/12.540048.

5. Krishna Chintalapudi, Jeongyeup Paek, Nupur Kothari, Sumit Rangwala, John Caffrey, Ramesh Govindan, Erik Johnson, Sami Masri, “Monitoring Civil Structures with a Wireless Sensor Network”, IEEE Internet Computing, March/April 2006.
6. Shamim N. Pakzad, Gregory L. Fenves, Sukun Kim, and David E. Culler, “Design and Implementation of Scalable Wireless Sensor Network for Structural Monitoring”, In ASCE Journal of Infrastructure Engineering, March 2008, Volume 14, Issue 1, pp. 89-101.