Security Aspects of Sensor Networks

[1]Mohd Muntjir, [2]Mohd Rahul, [3]Mohammad Asadullah
College of Computers and Information Technology
Taif University, Taif, Saudi Arabia

Abstract

Sensor networks are amassed wireless networks of small, low-cost sensors that collect and propagate environmental data. The emerging field of wireless sensor networks integrates sensing, computation, and communication into a single device. The power of wireless sensor networks verifies in the capability to deploy huge numbers of small nodes that collaborates and configure them. Wireless sensor networks simplify monitoring and handling of physical environments from remote locations with best accuracy. Security protocols associated to sensor network are analyzed in this paper.

Keywords: *Application areas, system evaluation metrics, sensor nodes, security protocols.*

1. Introduction

A sensor network is an integration of a large number of sensor nodes that are obtusely deployed either inside the anomaly or very close to it. Random deployment in inaccessible domain or disaster relief operations of sensors is done. Sensor nodes are assumable with an onboard processor. Instead of sending the raw data to the nodes incumbent for the fusion, they use their processing capacity to locally carry out simple computations and broadcast only the required and fractionally processed data [1].

Sensors associated into structures, machinery, and the environment, conjugated with the efficient delivery of sensed information, could provide extraordinary benefits to society. Potential benefits append: minor catastrophic failures, conservation of natural resources, elaborated manufacturing fertility, improved emergency response and enhanced homeland security. However, barriers to the outspread use of
sensors in structures and machines remain. Bunches of lead wires and fiber optic “tails” are subject to wreckage and connector failures. Long wire bundles personify a expressing installation and long term preservation cost, limiting the number of sensors that may be dispose and accordingly reducing the total quality of the data revealed. Wireless sensor networks can discard these costs, easing installation and dismissing connectors. The ideal wireless sensor is networked and supplying, consumes very little power, is smart and software programmable, capable of fast data possession, reliable and genuine over the long term, costs short to take and install, and requires no real conservation. Selecting the ideal sensors and wireless communications link requires knowledge of the application and obstacle definition. Battery life, sensor update rates, and size are all extensive design deliberation. Examples of low data rate sensors combine temperature, humidity, and maximize strain captured peacefully. Examples of high data rate sensors combine strain, acceleration, and vibration. The way of wireless sensor networks is based on a simple equation;

Sensing + CPU + Radio = Thousands of potential applications
As soon as the people distinguish the capabilities of a wireless sensor network, hundreds of applications buck to mind. It looks like a genuine combination of modern technology. A wireless sensor network (WSN) extensively consists of a base station (or “gateway”) that can communicate with a number of wireless sensors via a radio link. Data is poised at the wireless sensor node, compressed and send to the gateway straightly or, if required, uses other wireless sensor nodes to forward data to the gateway. After this the transmitted data is then given to the system by the gateway connection. The total aim of this chapter is to given a brief technical introduction to wireless sensor networks and existent a few applications in which wireless sensor networks are enabling.

2. WIRELESS SENSOR NETWORK ARCHITECURE

There are lots of different topologies for radio communications networks. A concise discussion of the network topologies that apply to wireless sensor networks are defined below.

A. Star Network (Single Point-to-Multipoint):

The star topology is useful in WSN, mainly in the development of Wireless Body Area Networks (WBAN).In this topology, a central node has the responsibility of the allocation with the medical sensors and the communication outside the BAN. The advantage of this type of network for wireless sensor networks is in its clarity and the ability to keep the remote node‟s power desolation to a minimum. It also allows for low suspension communications between the remote node and the base station. The deprivation of such a network is that the base station must be within radio transmission range of all the individual nodes and is not as fit as other networks in view of its dependency on a single node to conduct the network. The star network topology is as usual used in Body Area Networks (BAN), also called Body Sensor Network (BSN), where sensors are allocated on the body of a specimen.

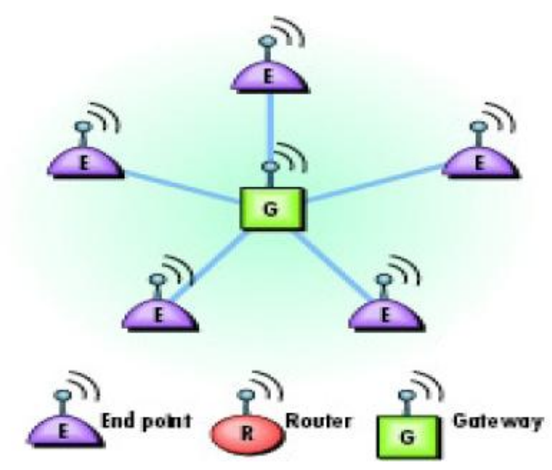

Fig. 1: Star Network

B. Mesh Network:

A mesh network allocates for any node in the network to broadcast to any other node in the network that is within its radio transmission domain. This network topology has the favor of redundancy and reliability. If a particular node fails, a remote node still can telecast to any other node in its range, can forward the message to the desired location. In this way, the range of the network is not limited by the range in between single nodes; it can simply be enlarged by adding more nodes to the system.

The disadvantage of this type of network is in power depletion for the nodes that implement the multichip communications are extensively higher than for the nodes that don‟t have this potential, generally limiting the battery life. Furthermore, as the number of communication mingle to destination increases; the time to redeem the message also increases, primarily if low power operation of the nodes is a requirement. The current enlargements in WSN are also centralizing on mesh network topology because it admits for the communication between devices without a central node for routing using a mesh of nodes. This feature discards the central failure, and contributes self-healing and self-organization.

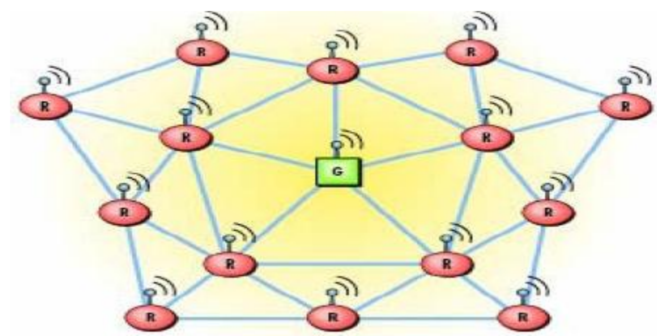

Fig. 2: Mesh Network

3. NETWORK APPLICATION AREAS

A. Applications Classification

It could be ordered into two categories: event detection (ED) and spatial process estimation (SPE). In event detection sensors are expanded to expose an event such as fire in a forest, a quake, etc. [2–3]. Signal processing within tools is very simple; each device has to compare the systematic quantity with a given inception and to send the binary information to the sink(s).

The density of nodes must assure that the event is detected and delivered to the sink(s) with a applicable probability of success while cultivating a low probability of wrong alarm. The detection of the phenomenon of interest (POI) could be finished in a decentralized (or dispensed) way.

In SPE the WSN intent at estimating a given physical phenomenon, that can be modeled as a bi-dimensional random process. It evaluates the all behavior of the spatial process based on the samples taken by sensors that are commonly placed in random positions [3–4].

4. SYSTEM EVALUATION METRICS

Meanwhile the key evaluation metrics for wireless sensor networks are full time, coverage, cost and ease of categorization, response time, physical accuracy, security, and effective sample rate.

A. Lifetime

Energy is the bounded factor for the lifetime of a sensor network. Each node must be designed to conduct its local supply of energy. Nodes can be evidently powered or self-powered.

B. Coverage

Multi-hop networking protocols elaborate the power consumption of the nodes, which may decline the network lifetime.

C. Cost and ease of deployment

Wireless sensor network must construct itself. All through the lifetime of a deployment, nodes may be dislocated or large physical objects may be arranged so that they interfere with the communication between two nodes.

In an actual deployment, a fragment of the total energy budget must be devoted to system maintenance and verification. The generation of characteristic and reconfiguration traffic deflates the network lifetime. This can also decreases the efficient sample rate.

D. Response Time

Although low power operation, nodes must be proficient of having immediate, high-priority messages communicated across the network as swiftly as possible response time must be as low as possible.

Network lifetime can be increased by having nodes only compelled their radios for limited periods of time but it reduces the responsiveness of system.

E. Temporal Accuracy

The network must be capable of constructing and maintaining a global time base that can be used to sequentially order fragments and events. In a distributed system, energy must be distributed to maintain this expanded clock.

The time synchronization information must be constantly communicated between nodes. The frequency of the synchronization messages is dependent on the aspired accuracy of the time clock.

F. Security

Encryption and cryptographic authentication are used for security but it charged both power and network bandwidth [8-9]. The extra computation must be achieved to encrypt and decrypt data and extra authentication bits must be transmitted with each and every packet.

G. Effective Sample Rate

Effective sample rate is denoted as the sample rate that sensor data can be taken at each and every sensor and communicated to an acquisition point in a data collection network.

In a data collection tree, a node must hold the data of all of its descendants. Network bit rates combined with maximum network size end up smashing the effective per node sample rate of the complete system [10].

Distinct forms of spatial and temporal compression can be used to reduce the communication bandwidth demanded while maintaining the same active sampling rate. Local storage can be used to collect and store data at a high sample rate for limited periods of time. The data can then be downloaded over the multi-hop network as bandwidth grants.

5. SENSOR NODES

Miniaturization, low power and low cost composed are likely the most exacting technical problem for sensor nodes.

A. Device Classes

Two forms of device classes are Commodity devices and Custom built nodes from commercially-available electronics segments.

1) Commodity Devices

Commercially available commodity devices are used to frame prototypical sensor network algorithms and functions. Commodity devices include laptop computers, PDAs, mobile phones, cameras.

Many commodity devices afford regulated wired and wireless interfaces and application protocols that allow using the device‟s serviceability without a extreme programming act.

2) COTS Sensor Nodes

CTOS abbreviates for the custom-built sensor nodes. COTS nodes are fabricated from several commercially off-the shelf (COTS) electronic components. COTS node expansion provides an adaptable, commonly applicable sensor node.

A classical setup consists of an RF transceiver and antenna, one or more sensors, as well as a battery and power regulating circuitry collected around a general-purpose processor.

Those processors are often 8-bit microcontrollers having internal memory, remains with some additional external memory.

3) Sensor-Node Systems-on-a-Chip

The research groups have recently oppressed the development of whole sensor-node systems-on-a-chip (SOC). Such designs collaborate most (if not all) sensor-node subsystems on a single die or multiple dies in one package. This integrates microcontrollers and memories but also novel sensor designs as well as wireless receivers and transmitters. Examples of sensor-node SOCs are Smart Dust, the Spec Mote, and SNAP.

B. Sensor-Node Components

1) Processors

Sensor node designs have 8-bit RISC microcontroller as their major processor. The microcontroller may also have to handle a simplistic RF radio.

The computational power of 8- bit microcontrollers is often as limited as to perform complex tasks, some sensor nodes designs use 16 or even 32-bit microcontroller, or they have additional ASICs, DSPs, or FPGAs.

2) Memories

Sensor nodes are generally based on microcontrollers that generally have Harvard architecture.

Maximum novel microcontroller designs feature constructed data and instruction memories, but do not have a memory management unit (MMU) and thus cannot enhance memory security. Mostly the sensor-node designs to add external data memory or nonvolatile memory just like as FLASH-ROM.

Microcontrollers used in COTS sensor nodes accommodate between 8 and 512 Kbytes of non-volatile program memory and up to 4 Kbytes of volatile SRAM. Memory absorbs a significant fraction of the chip; the die area is a commanding cost factor in chip design.

3) Wireless Communication Subsystems

Numerous sensor networks utilize radio frequency (RF) communication; even light and sound have also been engaged as physical communication medium. Sensors, Sensor Boards and Sensor Interface:

All the sensor node constructs are Application-specific, General-purpose node design are minor with external interfaces. The external interface grants to connect different sensors or actuators precisely or to attach a preconfigured sensor board.

The sensors-node constructs are for visible light, infrared, audio, pressure, temperature, acceleration, position (e.g., GPS).

Fewer common sensor types integrate hygrometers, barometers, magnetometers, oxygen saturation sensors, and heart-rate sensors. Simple analog sensors are inspected by the processor via an analog-to-digital converter (ADC).

6. SECURITY PROTOCOLS IN SENSOR NETWORKS

A. Key Management

Key management is foremost to assure purity of sensor data and protected communication through cryptographic techniques random key pre-distribution and localized encryption and authentication protocol. RKP (Random Key Pre-distribution) RKP schemes have many variants.

Eschenauer and Gligor [16] propose a key pre-distribution scheme that commits on probabilistic key allocation among nodes within the sensor network.

These system works by circulating; a key ring to each and every participating node in the sensor network before formation. RKP scheme is distributed into three states: first one is key setup and next is shared-key discovery, and third one is path-key establishment. And thus it contributes the key revocation phase.

• *Key Setup*

Each node‟s key ring responds of a number of randomly chosen keys from a big pool of keys developed offline.

The purpose of key setup phase is to confirm that a limited number of keys are accessible to probabilistically create a common key between two or more sensors during shared key discovery phase.

• *Shared-key Discovery*

Each node telecast a key identifier list, and compares the list of identities collected to the keys in their key chains.

• *Path-key Establishment*

A node tries to connect through intermediate nodes that already have a link established through the preceding phase.

• *Key Revocation*

An arbitrated sensor node can be reason for a lot of damage to the network. So retraction of a compromised node is very useful in key distribution scheme.

When a node is compromised by an antagonist, the key ring must be deleted. Each and every neighbor should delete the key of a compromised node from their key circle. LEAP (Localized Encryption and Authentication Protocol) developed by Zhu et al. (2003) as a key management protocol for sensor networks [14]. Featherweight, energy sufficient operation and robustness and survivability are the major design targets of this protocol.

A standard implementation of LEAP (LEAP+) was configured on the Berkeley Mica2 motes [15]. RC5 is uses by the protocol for encryption and CBC-MAC for authentication.

Four different keying mechanisms provided by LEAP:

1) Individual Keys, 2) Group Keys, 3) Cluster Keys and 4) Pair wise Shared Keys.

The Individual Key is a unique key that each and every node shares with the base station. This permits for private communication between the base station and individual nodes, useful for important instructions or keying material etc.

The Group Key is a publically shared key that is adopted by the base station for sending encrypted messages to the whole sensor network (or Group). This may be treated to send queries or interests, or to generate a mission to the nodes of the network.

A Cluster Key is identical but is shared between a node and its neighbors. This is generally employed for securing private broadcast messages (routing information or enabling passive participation) [13].

A Pair wise Shared Key is a key which every node shares with each of its current neighbors.

These keys are used under this scheme for protected communications that demand privacy or source authentication. It could also use this key to disperse a Cluster Key, for example. The use of these keys includes reserved participation.

B. Cryptography & Authentication

TINYSEC Karlof et al. (2004) designed the replacement for the deficient SNEP, known as TinySec and a “Link Layer Security Architecture for Wireless Sensor Networks” [13]. This affords services as like access control, message integrity and confidentiality and scalability.

Access control and integrity are assumed through authentication and confidentiality through encryption. Semantic security is acquired through the use of a different initialization vector (IV) for each invocation of the encryption algorithm. TinySec grants for two specific variants:

TinySec-Auth, affords for authentication only, and the second, TinySec-AE, affords both authentication and encryption. For TinySec-Auth, the whole packet is authenticated using a MAC, but the charged data is not encrypted; although using authenticated encryption, TinySec encrypts the charged data and then authenticates the packet with a MAC.

The Security Protocols for Sensor Networks (SPINS) [11] activity possess of two main threads of work: an encryption protocol for Smart Dust motes called Secure Network Encryption Protocol (SNEP) and a telecast authentication protocol that is called micro-Timed Efficient streaming learnt Authentication (TESLA).

In SPINS, each sensor node contributes a different master key with the base station. On the other hand the keys required by the SNEP and the TESLA protocols are copied from this master key.

1) SNEP is based on Cipher Block Chaining implemented in the Counter mode (CBC-CTR), with the sense that the initial value of the counter in the sender and receiver is the same.

To achieve authenticated telecasts, TESLA uses a time-released key chain and gives authenticated cascading telecast, and SNEP (Secure Network Encryption Protocol) that provides data confidentiality and two edge data authentication, and data freshness with low overhead.

In Sensor Network Encryption Protocol (SNEP) the encrypted data has the following format: $E = \{D\}(Kencr, C)$, where D is the data and encryption key is $Kencr$ and the counter is C. The MAC is $M = MAC(Kmac, C|E)$.

The both keys $Kencr$ and $Kmac$ are derived from the master secret key K. The whole message that A sends to B is: $A\_B : \{D\}(Kencr,C),MAC(Kmac,C|\{D\}(Kencr,C))$. SNEP has attributes like Semantic security and Data authentication, Replay protection, Weak freshness and Low communication overhead.

2) µTESLA compete asymmetry through the delayed disclosure of symmetric keys and serves as the telecast authentication service of SNEP.

µTESLA requires that the base station and the nodes be closely time synchronized and each node knows an upper bound on the biggest error for synchronization.

The base station calculates a MAC on the packet with a key that is secret at that point in time. When a node gets a packet, it can assure that the base station did not yet display the corresponding MAC key, using its closely synchronized clock, maximum synchronization error and the time at which the keys are to be revealed.

The node reserves the packet in a buffer and aware that the MAC key is only known to the base station, and that no opponent could have fixed some packets during the transmission. When the keys are to be displayed, the base station telecasts the key to each and every receiver.

The receiver can then authenticate the righteousness of the key and use it to authenticate the packet in the buffer [11].

Each MAC key from the keys is a member of a key chain that has been created by a one way function F. According to generate this chain, the sender elects the end key, Kn, of the chain at random and applies F regularly to compute all other keys:

Ki = F(Ki+1)

Utilizing the SNEP building block, each node can smoothly dispose time synchronization and deliver an authenticated key from the key chain for the "commitment in a protected and authenticated manner" [12].

7. CONCLUSION

This paper will help the person to know in detail about the sensor network and about the security protocols for WSNs: RKP, LEAP, TinySec, SPINS used in sensor network.

The above work emphasis our preliminary work related to the security protocols. Open-source implementations of the protocols are in the process of being made available for work. LEAP includes collapses and what we do claim is that LEAP is a very good solution. The LEAP protocols are shortly available for the industry needs otherwise they can grow into a best solution. Currently, as for wireless sensor networks, TinySec is a very important expanded protocol for data link security. In this paper work a smooth key update scheme for TinySec is given based on the weight synchronization model.

References

[1] Akyildiz, I.; Su, W.; Sankarasubramaniam, Y.; Cayirci, E. A survey on sensor networks. IEEE Commun. Mag. 2002, 40, 102–114.

[2] Lucchi, M.; Giorgetti, A.; Chiani, M. Cooperative Diversity in Wireless Sensor Networks. In Proceedings of WPMC‟05, Aalborg, Denmark, 2005, pp. 1738–1742.

[3] Toriumi, S.; Sei, Y.; Shinichi, H. Energy-efficient Event Detection in3DWireless Sensor Networks. In Proceedings of IEEE IFIP Wireless Days, Dubai, United Arab Emirates, 2008.

[4] Behroozi, H.; Alajaji, F.; Linder, T. Mathematical Evaluation of Environmental Monitoring Estimation Error through Energy-Efficient Wireless Sensor Networks. In Proceedings of ISIT, Toronto, Canada, 2008.

[5] Perrig, A., et al., SPINS: Security protocols for sensor networks. Proceedings of MOBICOM, 2001, 2002.

[6] Rivest, R., The RC5 Encryption Algorithm. 1994: Fast Software Encryption. p.86-96.

[7] Doherty, L., Algorithms for Position and Data Recovery in Wireless Sensor Networks. UC Berkeley EECS Masters Report, 2000.

[8] A. Perrig, R. Szewczyk, V.Wen, D. Culler, and J. D. Tygar. SPINS: Security Protocols for Sensor Networks. Wireless Networks Journal (WINET), 8(5):521.534, September 2002.

[9] Deng, J., Han, R., Mishra, S. (2004) „Intrusion Tolerance and Anti- Traffic Analysis Strategies for Wireless Sensor Networks‟, The International Conference on Dependable Systems and Networks, 1 July, 2004, Florence, Italy.

[10] Karlof, C., Sastry, N., Wagner, D. (2004) „TinySec: A Link Layer Security Architecture for Wireless Sensor Networks‟, Proceedings of the 2nd International Conference on Embedded Networked Sensor Systems, Baltimore, MD, USA, 03 – 05 November 2004, New York, NY, USA: ACM Press, 162 – 175.

[11] Zhu, S., Setia, S., Jajodia, S. (2003) „LEAP: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks‟, CCS ‟03, Washington D.C., USA, 27 – 31 October 2003, New York, USA: ACM Press, 62-72.

[12] Zhu, S., Setia, S., Jajodia, S. (2006) „LEAP+: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks‟, ACM Transactions on Sensor Networks TOSN, 2(4), 500-528.

[13] L. Eschenauer and V.D. Gligor, "A key management scheme for distributed sensor networksm" In Proceddings of the 9th ACM conference on Computer and communications security, pp. 41-47, Nov. 2002.