Next Generation Network: Security and Architecture

Prof. Purvi G. Trivedi [1] Prof. Hardik D. Patel [2] Prof. Amit N. Patel[3]
[1, 2, 3]Department of Computer Science
[1, 2]S.S. College of Engg.
[1, 2, 3]Ganpat University, Kherva, Gujarat, India

Abstract— Wireless sensor networks will be widely deployed in the near future. While much research has focused on making these networks feasible and useful, security has received little attention. Wireless Sensor Networks (WSN) are a most challenging and emerging technology for the Research due to their vital scope in the field coupled with their low processing power and associated low energy. As wireless sensor networks continue to grow, so does the need for effective security mechanisms. Because sensor networks may interact with sensitive data and/or operate in hostile unattended environments, it is imperative that these security concerns be addressed from the beginning of the system design staring with a brief overview of the sensor networks security, a review is made of and how to provide the security in the wireless sensor networks. This paper studies the security problems, Requirement, Architecture of WSN and different platform, characterized by severely constrained computational and energy resources, and an ad hoc operational environment.

Keywords: Sensor, Security, Architecture, Different platform.

I. INTRODUCTION

The basic idea of sensor network is to disperse tiny sensing devices; which are capable of sensing some changes of incidents/parameters and communicating with other devices, over a specific geographic area for some specific purposes like target tracking, surveillance, environmental monitoring etc. Today's sensors can monitor temperature, pressure, humidity, soil makeup, vehicular movement, noise levels, lighting conditions, the presence or absence of certain kinds of objects or substances, mechanical stress levels on attached objects, and other properties We classify the main aspects of wireless sensor network platform and architectures. Wireless sensor networks are collection of nodes where each node has its own sensor, processor, transmitter and receiver and such sensors usually are low cost devices that perform a specific type of sensing task. Security is a common concern for any network system, but security in Wireless Sensor Network is of great importance to ensure its application success. For example, when sensor network is used for military purpose, it is very important to the sensed information confidential and authentic. Providing security for WSN represents a rich field of research problems as many existing security schemes for traditional networks are not applicable for WSN. Sensor networks refer to a heterogeneous system combining tiny sensors and actuators with general-purpose computing elements. These networks will consist of hundreds or thousands of self-organizing, low-power, low-cost wireless nodes deployed en masse to monitor and affect the environment. Potential applications include burglar alarms, inventory control, medical monitoring and emergency response [3], monitoring remote or inhospitable habitats [1, 2], target tracking in battlefields [4], disaster relief networks, early fire detection in forests, and environmental monitoring.

II. BASIC SECURITY IN NGN

Security is a broadly used term encompassing the characteristics of authentication, integrity, privacy, No repudiation and anti-playback [5]. The more the dependency on the information provided by the networks has been increased, the more the risk of secure transmission of information over the networks has increased. A next-generation network integrates security capabilities from the premise to the cloud. Integration means less administrative overhead and fewer security gaps.

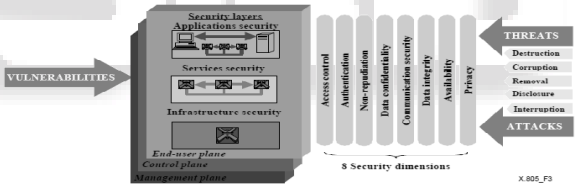

Fig. 1: Security Architecture of NGN
(ITU-T Recommendation X.805)

A. *Cryptography*

The encryption-decryption techniques devised for the traditional wired networks are not feasible to be applied directly for the wireless networks and in particular for wireless sensor networks. WSNs consist of tiny sensors which really suffer from the lack of processing, memory and battery power [6], [7], [8], [9]. Applying any encryption scheme requires transmission of extra bits, hence extra processing, memory and battery power which are very important resources for the sensors' longevity. Applying the security mechanisms such as encryption could also increase delay, jitter and packet loss in wireless sensor networks [10]. Moreover, some critical Questions arise when applying encryption schemes to WSNs like, how the keys are generated or disseminated. How the keys are managed, revoked, assigned to a new sensor added to the network or renewed for ensuring robust security for the network. As minimal (or no) human interaction for the sensors, is a fundamental feature of wireless sensor networks, it becomes an important issue how the keys could be modified time to

time for encryption. Adoption of pre-loaded keys or embedded keys could not be an efficient solution.

B. Steganography

While cryptography aims at hiding the content of a message, steganography [11], [12] aims at hiding the existence of the message. Steganography is the art of covert communication by embedding a message into the multimedia data (image, sound, video, etc.) [13]. the main objective of steganography is to modify the carrier in a way that is not perceptible and hence, it looks just like ordinary. It hides the existence of the covert channel, and furthermore, in the case that we want to send a secret data without sender information or when we want to distribute secret data publicly, it is very useful. However, securing wireless sensor networks is not directly related to steganography and processing multimedia data (like audio, video) with the inadequate resources [14] of the sensors is difficult and an open research issue.

C. Physical Layer Secure Access

Physical layer secure access in wireless sensor networks could be provided by using frequency hopping. A dynamic combination of the parameters like hopping set (available frequencies for hopping), dwell time (time interval per hop) and hopping pattern (the sequence in which the frequencies from the available hopping set is used) could be used with a little expense of memory, processing and energy resources. Important points in physical layer secure access are the efficient design so that the hopping sequence is modified in less time than is required to discover it and for employing this both the sender and receiver should maintain a synchronized clock. A scheme as proposed in [15] could also be utilized which introduces secure physical layer access employing the singular vectors with the channel synthesized modulation.

III. SECURITY DIMENSIONS AND MECHANISMS (BASED ON ITUT X.805)

Wireless Sensor Network is vulnerable to various attacks like any other conventional network, but its limited resource characteristics and unique application features requires some extra security requirements including the typical network requirements. [19] [18] [17] discuss on several security properties that should be achieved when designing a secure WSN.

A. Data Confidentiality

Data confidentiality is one of the vital security requirements for WSN because of its application purpose (for example, military and key distribution applications). Sensor nodes communicate sensitive data, so it is necessary to ensure that any intruder or other neighboring network could not get confidential Information intercepting the transmissions. One standard security method of providing data confidentiality is to encrypt data and use of shared key so that only intended receivers can get the sensitive data. Section 5 discusses more on this cryptography issues for WSN.

B. Authentication

Next Generation Networks (NGN) provides multimedia services to mobile users through different access networks including WLAN. The security architecture of NGN specifies that a WLAN user must follow a multi-pass Authentication and Key Agreement (AKA) procedure, in order to get access to the IP multimedia subsystem (IMS) services. This includes a repetition of authentication steps and protocols which introduce an unnecessary overhead.

C. Availability

We cannot ignore the importance of availability of nodes when they are needed. For example, when WSN is used for monitoring purpose in manufacturing system, unavailability of nodes may fail to detect possible accidents. Availability ensures that sensor nodes are active in the network to fulfill the functionality of the network. It should be ensured that security mechanisms imposed for data confidentiality and authentication are allowing the authorized nodes to participate in the processing of data or communication when their services are needed. As sensor nodes have limited battery power, unnecessary computations may exhaust them before their normal lifetime and make them unavailable. Sometimes, deployed security protocols or mechanisms in WSN are exploited by the adversaries to exhaust the sensor nodes by its resources and makes them unavailable for the network.

So, security policies should be implied so that sensor nodes do not do extra computation or do not try to allocate extra resources for security purpose.

D. Requirements for Secure Sensor Network Protocols

The above mentioned security requirements are the basic security needs for WSN. However, sensor nodes are always at a risk of physically being captured. Only fulfilling those basic Requirements cannot totally solve the security problems created by node compromise. Tamper resistance hardware can protect the data stored on sensor node. But using such hardware exceeds the cost limit of WSN by increasing cost of individual sensor node. So, a better solution is to design secure sensor network protocols that are resilient to node comprise or node failure. Secure protocols can also be developed to achieve the basic security requirements. Security protocols for WSN should have the capability of providing the following requirements besides the basic security requirements to ensure proper security functionality in WSN.

- *Data Freshness*

Data Freshness implies that the data is recent. This is an important security requirement to ensure that no message has been replayed meaning that the messages are in an ordering and they cannot be reused. This prevents the adversaries from confusing the network by replaying the captured messages exchanged between sensor nodes. To achieve freshness, security protocols must be designed in such a way that they can identify duplicate packets and discard them preventing replay attack.

- *Robustness against Attacks*

Security protocols should have robustness against attacks. If an attack is performed they should have the Ability to minimize the impact. They also should have the ability to detect failed sensor nodes and work with the remaining nodes and updated topology.

- *Resilience*

In practice, detection of compromised nodes and revocation of their cryptographic keys are not always possible. So, a

security protocol should always consider WSN with compromised nodes. If a number of nodes are compromised, secure protocols should function in such a way that the performance of WSN degrades gracefully.

– *Broadcast Authentication*

The base station broadcasts command and data to sensor nodes. An attacker can modify or forge the commands and sensor nodes perform incorrect operations accepting those commands. So, secure protocols should provide broadcast authentication functionality for the sensor nodes.

– *Self-Organization*

In WSN, there is no fixed network infrastructure as WSN is typically an ad hoc network. So, the sensor nodes must have the self-organizing and self-healing capability to support multi hop routing. But, secure communication among the sensor nodes is a precondition for providing security in WSN. So, security protocols should support efficient key management so that sensor nodes self-organize themselves according to the key distribution and can build trust relations with the neighbor nodes and secure virtual infrastructure as well.

– *Scalability*

The number of sensor nodes in WSN can be of several orders of magnitudes and the nodes are densely deployed. Again, the network topology of WSN is dynamic in nature that is new nodes can be added extending the network size. So, scalability is an important issue and security protocols as well as key management should cope with the increasing network size. A security mechanism is not an efficient one if it performs well in a small size network but does not work well for large size network.

– *Time Synchronization*

Most sensor network applications rely on some form of time synchronization. In order to conserve power, an individual sensor's radio may be turned off for periods of time. Furthermore, sensors may wish to compute the end-to end delay of a packet as it travels between two pair wise sensors. A more collaborative sensor network may require group synchronization for tracking applications, etc. In [20], the authors propose a set of secure synchronization protocols for sender-receiver (pair wise), multihop sender-receiver (for use when the pair of nodes are not within single-hop range), and group synchronization.

IV. BASIC ARCHITECTURE OF WIRELESS SENSOR NETWORK

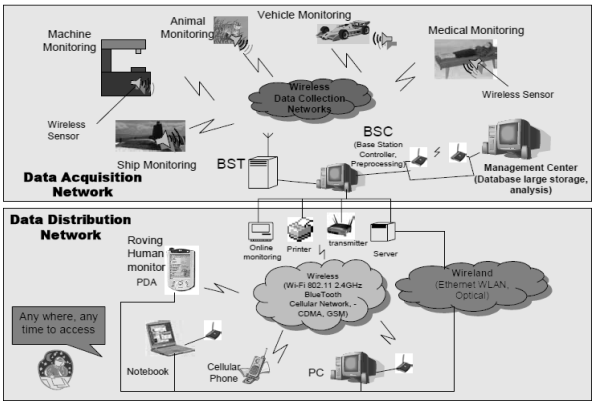

Fig. 2: Wireless sensor network architecture. [21]

The figure 2 shows the complexity of wireless sensor networks, which generally consist of a data acquisition network and a data distribution network, monitored and controlled by a management center. The plethora of available technologies makes even the selection of Sensor networks often have one or more points of centralized control called base stations. A base station is typically a gateway to another network, a powerful data processing or storage center, or an access point for human interface. They can be used as a nexus to disseminate control information into the network or extract data from it. Base stations have also been referred to as sinks. The sensor nodes establish a routing forest, with a base station at the root of every tree. Base stations are many orders of magnitude more powerful than sensor nodes. A sensor nodes communicate using RF, so broadcast is the fundamental communication primitive. The baseline protocols account for this property: on one hand it affects the trust assumptions, and on the other it is exploited to minimize the energy usage.

V. WIRELESS PLATFORMS

In addition to the collection of TinyOS related platforms discussed earlier, there are a collection of other wireless networking platforms that are relevant. Data on a single transmission channel. Link layer attack is the one part of DoS Attack by Collision Generation.

A. *Smart Dust*

The Smart Dust [22, 23] project at UC Berkeley represents the inspiration for much of the work contained in this thesis. The project has continued to develop miniature scale hardware structures that are advancing the state-of-the-art in wireless sensor network technology. In targeting extreme miniaturization and low-power consumption they are developing many ultra-low power primitives including the radio and ADC components contained on the Spec node. Additionally, the Smart dust project has pioneered new optical communication technologies through their use of MEMS mirror-based optical communication. By modulating reflected light, their corner cube reflector communication structure is able to transmit data across mile long links while consuming microwatts [24]. In addition to supporting the development of Spec, they have developed showcase devices that include sensing, computation, solar power sources, and optical communication. They have demonstrated autonomous sensor node that are less that 10 mm^3

B. *Bluetooth*

Bluetooth is a wireless system designed to be the industry standard for low power, mobile devices [25]. Highly integrated chipsets are being developed that provide RF circuitry and protocol processing on a single chip. While these designs will provide highly efficient implementations of the Bluetooth protocol, they will not provide the flexibility demanded by wireless sensor networks. Bluetooth has been designed as a wire replacement and includes support for very low-latency communication. To support low-latency and high-throughput operation, Bluetooth uses a channel hopping period of just 600 us. This requires all devices to remain synchronized to within a few

microseconds. In wireless sensor networks devices may only send data once per hour. It would be highly inefficient to force these nodes to remain synchronized for the entire hour. However, in Bluetooth it is expensive to enter and leave a network, it would be impractical for low duty cycle nodes to continually enter and leave a Bluetooth piconet. In a standard configuration, it takes over 2.4 seconds for connection establishment. During this time, the master node must be in a high-power scanning mode – typical Bluetooth radios consume hundreds of milliwatts wile monitoring the channel. Another incompatibility between wireless sensor networks and Bluetooth is that the master-slave topology of Bluetooth requires each slave to report to the master every few seconds. Again, this is not efficient for wireless sensor networks. While the Bluetooth chipsets are highly efficient and well integrated, their inability to provide lowpower operation modes makes it inefficient for wireless sensor networks.

C. Zigbee (802.15.4)

Zigbee is an industrial consortium designed to build a standard data link communication layer for used in ultra-low power wireless application [26]. The Zigbee alliance was formed because its members felt that existing standard technologies were not applicable to ultra-low power application scenarios. The Zigbee data link layer is designed to operate on top of the IEEE 802.15.4 physical layer [27]. IEEE 802.15.4 is a direct sequence spread spectrum physical layer including transmission bands at 868 MHz, 902-928 MHz and 2.4 GHz. First generation chipsets will be available in Q4 of 2003 [28]. Direct Sequence Spread Spectrum has a distinct advantage over channel hopping mechanisms because hop-sequence synchronization does not have to occur prior to initiating communication. This provides a large power advantage for low-duty cycle devices and addresses a major shortcoming of Bluetooth. Once completed, the Zigbee standard will specify a communication mechanism that is comparable to the AM communication layer provided in TinyOS. Primitive data framing mechanisms, error detection, and addressing will be standardized to allow compatibility. Zigbee is primarily focused on star topology networks where low-wireless devices communicated to powered collection point. A canonical Zigbee application is a174 wireless light switch. This would involve a low-cost battery operated switch communicating to a powered light fixture.

D. Pico Radio

There are several other groups looking into the architecture of wireless embedded devices. The Berkeley Wireless Research Center's PicoRadio project has identified the importance of application specific protocols, and has built a flexible platform by exploiting reconfigurable hardware [29]. The design incorporates reconfigurable building blocks that connect to their PicoRadio protocol processor, to give it the flexibility to implement a large number of underlying protocols. However, their overall node architecture does include a dedicated protocol processor and maintains a partition between protocol and application processing. The flexibility in protocol structure will still be limited by the protocol processors external interface.

E. Chipcon CC1010

Several radio manufactures have identified the benefits of integrating general purpose microcontroller onto the same CMOS die with the radio. One commercial part that has just become available is the Chipcon CC1010. It is the integration of a CC1000 transceiver and an Intel 8051 microprocessor. While they were able to bring the configuration registers of the radio onto the I/O bus of the CPU, they did not take the step of providing any additional integration to aid in the communication process. The data interface to the radio remains largely unchanged from what was possible when the microcontroller and radio are two separate chips we have demonstrated how the integration of CPU and radio on to a single chip creates new opportunities for interfaces between the radio and the CPU. However the simple form integration done by Chipcon in their CC1010 has simply reduced physical size and cost. The inclusion of communication accelerators are required to allow integration to yield significant performance improvements. The CC1010 does not realize the full potential that is allowed by our generalized architecture.

VI. CONCLUSION

In this paper we introduce, wireless sensor network Security, Architecture and different types of platform in detail. In sensor networks has been an increased singly important issue for both academia and in industry individuals and groups working in this fast growing research area. In a WSN, physical security of wireless links is virtually impossible because of the broadcast nature and resource limitation on sensor nodes and uncontrolled environments where they are left unattended. Consequently, security attacks on information flow can be widespread. While the platforms presented here are ready to meet the demands of real-world commercial applications, the technology enabling wireless sensor networks will continue to evolve. As advances in CMOS processes and RF radio technology are incorporated into next-generation wireless senor nodes, the power consumption and lifetime will continually improve. Currently, technology allows for multi-year operation off of a single pair of AA batteries. The upcoming technological advances will most likely be applied to decreasing the power consumption of the device. In turn, this will enable a reduction of physical size of the energy storage required for any given application. As for tighter levels of integration, the cost/size point represented by the Spec platform has reached the point of diminishing returns. Further reduction in the physical size of the radio, processing, and storage is no longer necessary. Only a select few applications have the need for a device that is smaller than 2.5 mm x 2.5 mm. However, all application scenarios can benefit from reduced power consumption which is translated into longer network lifetime and/or increased sample rates.

REFERENCES

[1]. Alan Mainwaring, Joseph Polastre, Robert Szewczyk, and David Culler.Wireless sensor networks for habitat monitoring. In First ACM International Workshop on Wireless Sensor Networks and Applications, 2002.

[2]. Robert Szewczyk, Joseph Polastre, Alan Mainwaring, and David Culler. Lessons from a sensor network expedition. In First European Workshop on Wireless Sensor Networks (EWSN '04), January 2004.
[3]. Matt Welsh, Dan Myung, Mark Gaynor, and Steve Moulton. Resuscitation monitoring with a wireless sensor network. In Supplement to Circulation: Journal of the American Heart Association, October 2003.
[4]. G.L. Duckworth, D.C. Gilbert, and J.E. Barger. Acoustic counter-sniper system. In SPIE International Symposium on Enabling Technologies for Law Enforcement and Security, 1996.
[5]. Undercoffer, J., Avancha, S., Joshi, A., and Pinkston, J., "Security for Sensor Networks", CADIP Research Symposium, 2002, available at, http://www.cs.sfu.ca/~angiez/personal/paper/sensor-ids.pdf
[6]. Perrig, A., Szewczyk, R., Wen, V., Culler, D., and Tygar, J. D., "SPINS: Security Protocols for Sensor Networks", Wireless Networks, vol. 8, no. 5, 2002, pp. 521-534.
[7]. Jolly, G., Kuscu, M.C., Kokate, P., and Younis, M., "A Low-Energy Key Management Protocol for Wireless Sensor Networks", Proc. Eighth IEEE International Symposium on Computers and Communication, 2003. (ISCC 2003). vol.1, pp. 335 - 340.
[8]. Rabaey, J.M., Ammer, J., Karalar, T., Suetfei Li., Otis, B., Sheets, M., and Tuan, T., "PicoRadios for wireless sensor networks: the next challenge in ultra-low power design" 2002 IEEE International Solid-State Circuits Conference (ISSCC 2002), Volume 1, 3-7 Feb. 2002, pp. 200 – 201
[9]. Hollar, S, "COTS Dust", Master's Thesis, Electrical Engineering and Computer Science Department, UC Berkeley, 2000.
[10]. Saleh, M. and Khatib, I. A., "Throughput Analysis of WEP Security in Ad Hoc Sensor Networks", Proc. The Second International Conference on Innovations in Information Technology (IIT'05), September 26-28, Dubai, 2005.
[11]. Kurak, C and McHugh, J, "A Cautionary Note on Image Downgrading in Computer Security Applications", Proceedings of the 8th Computer Security Applications Conference, San Antonio, December, 1992, pp. 153-159.
[12]. Mokowitz, I. S., Longdon, G. E., and Chang, L., "A New Paradigm Hidden in Steganography", Proc. of the 2000 workshop on New security paradigms, Ballycotton, County Cork, Ireland, 2001, pp. 41 – 50.
[13]. Kim, C. H., O, S. C., Lee, S., Yang, W. I., and Lee, H-W., "Steganalysis on BPCS Steganography", Pacific Rim Workshop on Digital Steganography (STEG'03), July 3-4, Japan, 2003.
[14]. Younis, M., Akkaya, K., Eltoweissy, M., and Wadaa, A., "On handlingQoS traffic in wireless sensor networks", Proc. of the 37th Annual Hawaii International Conference on System Sciences, 2004, 5-8 January, 2004, pp. 292 – 301
[15]. Orihashi, M., Nakagawa, Y., Murakami, Y., and Kobayashi, K., "Channel synthesized modulation employing singular vector for secured access on Physical layer", IEEE GLOBECOM 2003, Volume 3, 1-5 December, 2003, pp. 1226 – 1230.
[16]. Zhou, L. and Haas, Z. J., "Securing ad hoc networks", IEEE Network, Volume 13, Issue 6, Nov.-Dec. 1999, pp. 24 – 30.
[17]. E. Shi and A. Perrig. Designing secure sensor networks. In Wireless Communications, IEE, volume 11, December 2004
[18]. C.W. L.Weimin, Y. Zongkai and T. Ymmen. Research on the security in wireless sensor network. ˇTAsian Journal of Information Technology, 2006.
[19]. John PaulWalters, Zhengqiang Liang, Weisong Shi and Vipin Chaudhary. Wireless sensor network security: A Security in Distributed, Grid, and Pervasive Computing, 2006.
[20]. S. Ganeriwal, S. ˇCapkun, C.-C. Han, and M. B. Srivastava. Secure time synchronization service for sensor networks. In WiSe '05: Proceedings of the 4th ACM workshop on Wireless security, pages 97–106, New York, NY, USA, 2005. ACM Press.
[21]. http://arri.uta.edu/acs/networks/WirelessSensorNetChap 04.pdf
[22]. Atwood, B., B. Waraneke, and K.S.J. Pister. Preliminary circuits for smart dust. In Southwest Symposioum on Mixed-Signal Design. 2000. San Diego, Ca
[23]. Pister, K.S.J., J.M. Kahn, and B.E. Boser, Smart Dust: Wireless Networks of Millimeter-Scale Sensor Nodes. Electronics Research Laboratory Research Summary, 1999.
[24]. Chu, P.B., et al., Optical communication link using micro-macined corner cube reflectors. 1997: Proceeding of the SPIE vol. 3008-20.
[25]. The Official Bluetooth Website: http://www.bluetooth.com/.
[26]. ZigBee Alliance, The official website of the Zigbee Alliance: http://www.zigbee.org.
[27]. IEEE, IEEE 802.15 WPAN™ Task Group 4: http://ieee802.org/15/pub/TG4.html
[28]. Semiconductor, A., AMI Semiconductor First to Demonstrate Working ZigBee Wireless Device: http://www.amis.com/news/030414_zigbee.cfm
[29]. J.L. Da Silva Jr., J.S., M. J. Ammer, C. Guo, S. Li, R. Shah, T. Tuan, M. Sheets, J.M. Ragaey, B. Nikolic, A Sangiovanni-Vincentelli, P. Wright., Design Methodology for Pico Radio Networks. 2001, Berkeley Wireless Research Center. Authentication : NGN – Authentication in paper /NGN folder