International Journal of Management, IT & Engineering
Vol. 6 Issue 9, September 2016,
ISSN: 2249-0558 Impact Factor: 6.269
Journal Homepage: http://www.ijmra.us, Email: editorijmie@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gage as well as in Cabell’s Directories of Publishing Opportunities, U.S.A

SECURITY AND PRIVACY ISSUES AND SOLUTIONS FOR WIRELESS SYSTEM NETWORKS (WSN) AND RFID

RESHMA M

SHABEER T.K

Abstract

Recent advances in wireless networks and embedded systems have created a new class of pervasive systems such as Wireless Sensor Networks (WSNs) and Radio Frequency IDentification (RFID) systems. WSNs and RFID systems have provided promising solutions for a wide variety of applications. However, security and privacy concerns have raised serious challenges on these systems. These concerns have become more apparent when WSNs and RFID systems co-exist. In this article, we first briefly introduce WSNs and RFID systems. We then present their security concerns and related solutions. Finally, we propose a Linear Congruential Generator (LCG) based lightweight block cipher that can meet security co-existence requirements of WSNs and RFID systems.

Introduction

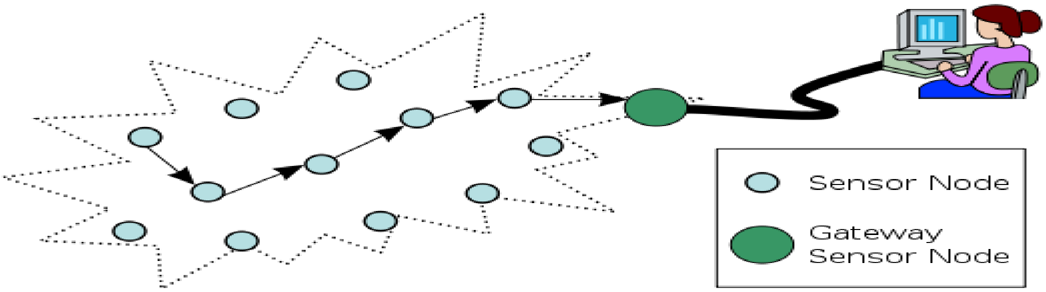
Recent advances in wireless networks and embedded systems have created a new class of pervasive systems such as Wireless Sensor Networks (WSNs) and Radio Frequency IDentification (RFID) systems. WSNs and RFID have made a variety of new and exciting applications viable. For example, WSNs have been used in areas such as health monitoring, scientific data collection, environmental monitoring, and military operations. RFID systems have become more and more popular to provide automatic identification systems in areas such as supply chain management, payment systems, manufacturing, and inventory control. The integration of WSNs and RFID systems has also opened up new opportunities in areas such as healthcare systems and wireless telemedicine.

WSNs usually comprise a large number of inexpensive, small, and battery-powered sensor nodes. Equipped with wireless communication modules and microcontrollers, each sensor node can monitor physical or environmental conditions, such as temperature, light, acoustic, etc., and collaborate to transmit data to a base station. WSNs are usually resource-constrained on processing power, memory, bandwidth, and energy consumption. For example, powered by AA batteries, MICA2 Motes consist of an 8 MHz 8-bit Atmel ATMEGA128L CPU with only 4KB RAM for data, 128KB program memory, 512KB flash memory, and 38.4kbps data rate ratio. RFID systems usually consist of simple and low-cost RFID tags, more powerful RFID readers, and a database which stores records associated with tag contents. Generally, a reader broadcasts an RF signal within a certain wireless range to access digital data stored in tags. Powered by a signal from an RFID reader or an internal battery, tags can respond to the reader by replying with information such as object identification data. Because tags are usually manufactured on a massive scale and any additional circuitry in tag design may incur extra cost, tags should be kept as lightweight as possible. For example, one tag in the form of Electronic Product Codes (EPC) may only contain 128-512 bits of read-only storage, 32-128 bits of volatile read-write memory, and 1, 000-10, 000 gates].

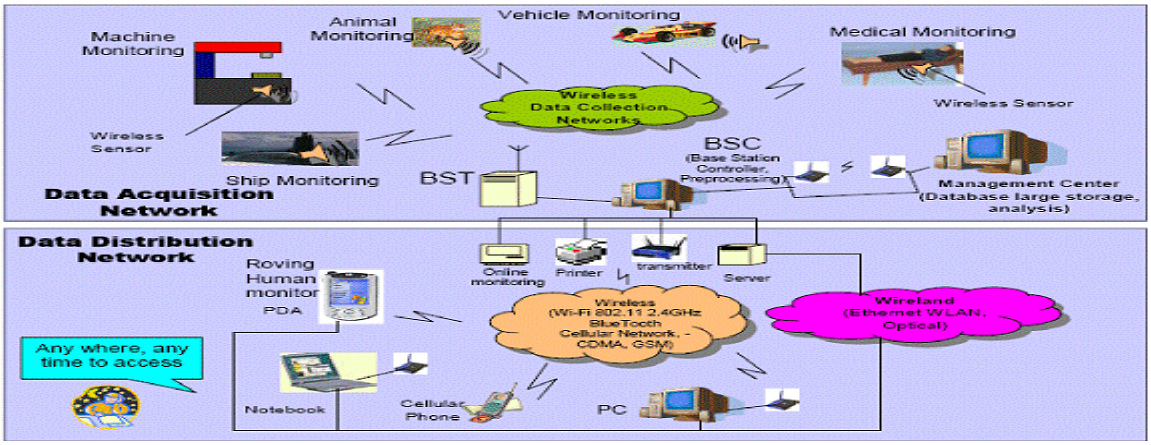
Unfortunately, the wide deployment of these low-cost devices is often subject to various kinds of attacks and thus raises serious security and privacy concerns. For example, WSNs are often deployed in untrusted or hostile environment such as battlefield to perform mission-critical tasks, in which an adversary can eavesdrop traffic, inject malicious messages, replay old messages, and so on. The pervasive deployment of tags makes RFID systems suffer from security threats such as tracking, hot listing, and profiling , which render tag data susceptible to an unauthorized reader and allow an adversary to gather private information illegally. The extreme resource-constrained nature of tags also makes it possible for attackers to insert a forgery or counterfeiting tag into an RFID system without being detected. All these vulnerabilities indicate that WSNs and RFID systems are not readily to be deployed for security-sensitive tasks without first addressing their security problems. Moreover, with the emergence of exciting applications such as wireless telemedicine, the co-existence of WSNs and RFID systems poses even more challenges for suitable security mechanisms. In this article, first briefly introduce WSNs and RFID systems. Then present their related security and privacy issues, as well as related solutions. Demonstrate that existing security solutions do not consider co-existence issues of WSNs and RFID systems. Finally, we propose a Linear Congruential Generator (LCG) based lightweight block cipher that can meet security co-existence requirements. Note that this article does not address integration issues (such as network architecture, networking protocols, etc.) of WSN and RFID systems. Instead, we aim at providing co-existent security solutions for such systems, i.e., we consider consistency and integration of security protocols.

Wireless Sensor Networks

One WSN may be composed of hundreds or thousands of miniature 2 Wireless sensor nodes, or motes, which are fitted with an on-board processor. The low-cost battery-powered sensor nodes have extremely limited energy supply, stringent processing and communications capabilities, and scarce memory. Sensor nodes are usually densely deployed in a sensor field in order to continuously monitor surrounding areas. In a sensor application, each sensor has the capability to collect data such as temperature, humidity, light condition, and so on, depending on targeted applications. After sensor nodes collect data, they can locally carry out some simple computations, and collaboratively route data to a base station for analysis. A base station may be a fixed node or a mobile node capable of connecting WSNs to a communications infrastructure (for example, the Internet) where users can have access to reported data. In order to reduce the amount of raw data transmitted to a base station and to save energy, sensor nodes often need to perform aggregation operations so that only processed information, for instance, the mean, max, or min of sensed raw data, is transmitted.



The WSN is built of "nodes" – from a few to several hundreds or even thousands, where each node is connected to one (or sometimes several) sensors. Each such sensor network node has typically several parts: a radio transceiver with an internal antenna or connection to an external antenna, a microcontroller, an electronic circuit for interfacing with the sensors and an energy source, usually a battery or an embedded form of energy harvesting. A sensor node might vary in size from that of a shoebox down to the size of a grain of dust, although functioning "motes" of genuine microscopic dimensions have yet to be created. The cost of sensor nodes is similarly variable, ranging from a few to hundreds of dollars, depending on the complexity of the individual sensor nodes. Size and cost constraints on sensor nodes result in corresponding constraints on resources such as energy, memory, computational speed and communications bandwidth. The topology of the WSNs can vary from a simple star network to an advanced multi-hop wireless mesh network

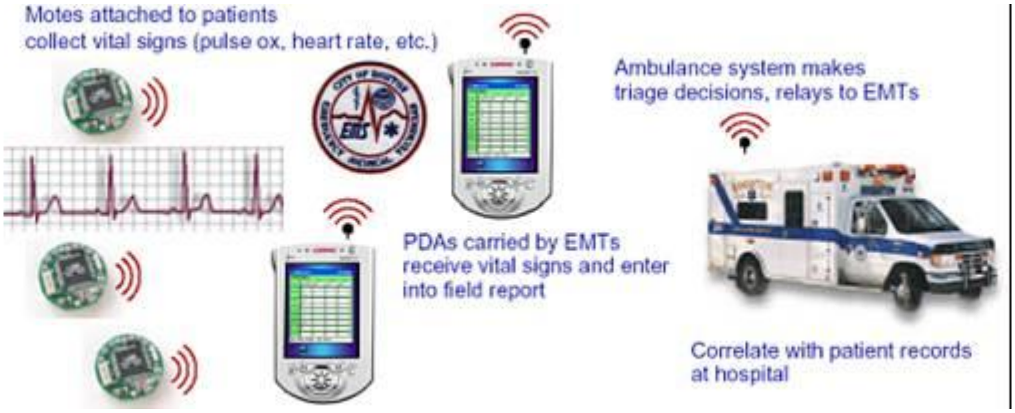


Application

Area monitoring

monitoring is a common phenomenon is to be monitored. A military example is the use of sensors detect enemy intrusion; a civilian example is the of gas or oil pipelines.

Health care devices are those that are inserted inside human body. There are many other applications too e.g. **monitoring** The medical applications can be of two types: wearable and implanted. Wearable devices are used on the body surface of a human or just at close proximity of the user. The implantable medical body position measurement and location of the person, overall monitoring of ill patients in hospitals


Motes attached to patients collect vital signs (pulse ox, heart rate, etc.)
Ambulance system makes triage decisions, relays to EMTs
PDAs carried by EMTs receive vital signs and enter into field report
Correlate with patient records at hospital

2.1 Security and Privacy Issues and Solutions for WSNs

The lack of physical security combined with unattended operations make sensor nodes prone to a high risk of being captured and compromised. The wireless broadcast nature may result in privacy breaches of sensitive information during data transmission. Therefore, security and privacy issues of WSNs have attracted a lot of research efforts. In the following, we list a brief taxonomy of WSN attacks and their representative solutions.

2.1.1 Attacks

- **Physical Attacks**: Sensor nodes may be left unattended for a long time. Therefore, attackers may have a high chance to compromise WSN nodes. From the hardware perspective, attackers can gain complete access to microcontrollers in sensor nodes and thus obtain sensitive information stored in node memory. From the software perspective, TinyOS, the most widely used Operating System in WSNs, and various applications may also suffer from well-know exploitations such as buffer overflow. All these enable attackers to extract relevant secrets, and insert malicious data to the network very easily.

• **Attacks at Physical Layer**: Jamming is one of the most important attacks at physical layer. Aiming at interfering with normal operations, an attacker may continuously transmit radio signals on a wireless channel. Equipped with a powerful node, an attacker can send high-energy signals in order to effectively block wireless medium and to prevent sensor nodes from communicating. This can lead to Denial-of-Service (DoS) attacks at the physical layers.

• **Attacks at Link Layer**: The functionality of link layer protocols, such as those specified in 802.15.4/ZigBee standards, is to coordinate neighboring nodes to access shared wireless channels and to provide link abstraction to upper layers. Attackers can deliberately violate predefined protocol behaviors at link layer. For example, attackers may induce collisions by disrupting a packet, cause exhaustion of nodes' battery by repeated retransmissions, or cause unfairness by abusing a cooperative MAC-layer priority scheme]. All these can lead to DoS attacks at the link layers.

• **Attacks at Network Layer:** In WSNs, attacks at routing layer may take many forms. For example, routing control packets exchanged among sensor nodes can be spoofed, replayed, or altered. In this way, routing logic can be compromised. Data packets may also be selectively dropped, replayed, or modified by compromised nodes. Besides these, WSNs also suffer from wormhole and sinkhole attacks, in which messages may be lured or tunneled to a particular area through compromised nodes. Attackers may also launch Sybil attack. Therefore, a single node may present multiple identities to other nodes in a network.

3 Radio Frequency Identification Systems

Envisioned as a replacement for barcodes, billions of RFID tags have been deployed on the market for various applications. For example, pharmaceutical companies have embedded RFID chips in drug containers to track the theft of highly controlled drugs. Airline companies may use RFID tags to track and route passenger bags. In all these applications, a tag is attached to a physical object and contains a digital number associated with that object. RFID *readers* broadcast a radio signal which contains an identifier in order to locate the object. Based on different operating frequencies (for example, 13.56 MHz or 915 MHz), RFID systems may have different reading ranges (for example, 1m or 3m). Because many RFID tags may be in the range of a reader at the same time, collisions may happen. Collision-avoidance protocols, such as *binary tree walking* protocol , are thus proposed to resolve this collision.

The pervasive nature of RFID systems make stored data increasingly distributed among different parties. This raises many new privacy and security for RFID systems. Because a reader is little more than a radio transceiver, it is thus relatively easy for attackers to obtain illegitimate readers and to query RFID tags for sensitive information. For example, consumer products labeled with insecure tags may reveal private information when queried by unauthorized readers. Many RFID protocols have no explicit authentication procedures. This may result in serious privacy concerns.rfid consist of a tag and areader relies on the electromagnetic signal from a reader to power its activity. An active tag includes an EPC is a simple, compact “license plate” that uniquely identifies objects (items, cases, pallets, locations, etc.) in the supply chain

EPC-RFID technology consists of two components: interrogators or readers and tags. A tag consists of three parts:

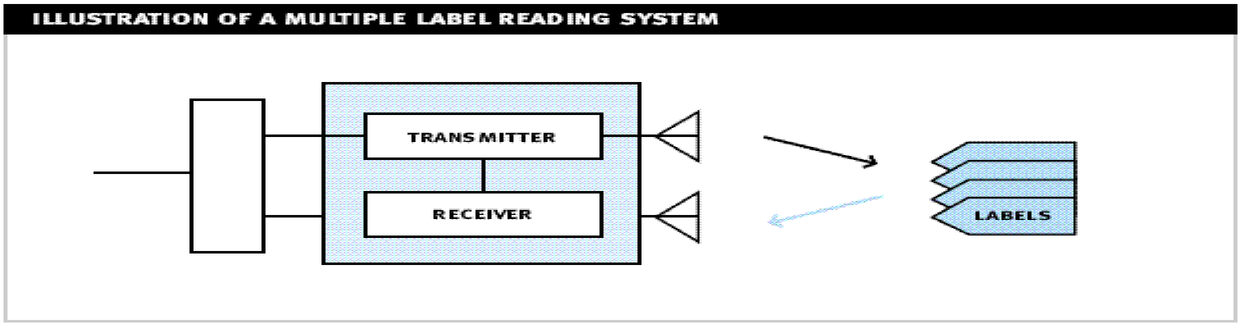
1. An integrated circuit for storing the EPC data.
2. An antenna.
3. A surface to place the tag in order to affix it onto an object.

Only EPC and security data is stored on the tag, this data is given meaning thorough association with other information within a company's supply chain database systems. The functions required for a tag are:

1. Being programmed with EPC data, CRC, destroy code and optionally other data

2. Being read by a interrogator
3. Being selected as a part of a related group of tags
4. Being individually destroyed (data destruction, not physical) Tags can either be passive, the most common, or active. A passive tag is unpowered attached battery for self-powered communication.

A reader is a device that reads or writes the EPC data to a tag. Readers would be placed at key points in a supply chain that make the most business sense to track movements of items. Readers may be fixed in location to monitor a stream of moving products or can be used as a mobile device. Hundreds of tags are expected to be able to be read per second by a single reader. The reader protocol uses Amplitude Shift Keying (ASK) in encoding signals and Direct Sequence Spread Spectrum in sending signals to tags. The tags themselves do not use DSSS in their communication to a reader but use the frequency on which they received a transmission from the reader.



The use of Radio Frequency Identification technology is very common. RFID is used in remote keyless entry in cars, garage door openers, Exxon Mobile's Speedpass gasoline payment system, airplane traffic identification systems, mobile phones (CDMA) and Wi-Fi wireless internet access to name a few general applications. All these technologies use electromagnetic waves through free space communication for unique identification purposes, which broadly qualifies them as RFID technologies. The key applications for which RFID is suited involve transportation, movement in time and space – thus locating and tracking the moving objects, and security, uniquely identifying your-self or an object

3.1 Security and Privacy Concerns for RFID

Because identifiers of RFID tags may be static and never change, this facilitates *tracking* attacks - to enable an attacker to track the movement of products. An adversary can also *hotlist* important objects, based on which activities of targeted objects can be *profiled* . RFID systems also suffer from *tag spoofing* and *cloning*, in which an adversary can physically access tags or use an unauthorized reader to read tags in order for spoofing. This allows an adversary to clone targeted tags.

Conclusions

In this article, we first briefly introduce WSNs and RFID systems. We then present their privacy and security concerns and related solutions. Also the attacks in WSN networks and RFID.

References

[1] Y. Xiao, X. Shen, B. Sun, and L. Cai, “Security and Privacy in RFID and Applications in Telemedicine,” *IEEEn Comm. Mag.*, Apr., 2006, pp. 64-72.

[2] B. Sun, C.-C Li, K. Wu, and Y. Xiao, “A Lightweight Secure Protocol for Wireless Sensor Networks,” *Elsevier Computer Communications Journal Special Issue on Wireless Sensor Networks: Performance, Reliability, Security, and Beyond*, 2006, pp. 2556-2568.

[3] D. Molnar and D. Wagner, “Privacy and Security in Library RFID: Issues, Practices, and Architectures,” *ACM CCS’04*, Washington, DC, USA, Oct. 2004, pp. 210-219.

[4] T. Dimitriou, “A Lightweight RFID Protocol to Protect Against Traceability and Cloning Attacks,” *IEEE SecureComm’ 05*, Athens, Greece, Sept. 2005, pp. 59-66.

[5] Stephen A. Weis, "New Foundations for Efficient Authentication, Commutative Cryptography, and Private Disjointness Testing," Ph.D. Dissertation, MIT, May 2006.

[6] Y. Xiao, H.-H Chen, B. Sun, R. Wang, and S. Sethi, "MAC Security and Security Overhead Analysis in the IEEE 802.15.4 Wireless Sensor Networks," *EURASIP Journal on Wireless Communications and Networking*, Article ID 93830, 2006.

[7] C. Karlof, N. Sastry, and D. Wagner, "TinySec: A Link Layer Security Architecture for Wireless Sensor Networks," *ACM Sensys'04*, Baltimore, MD, 2004, pp. 162-175.

[8] H. Song, S. Zhu, and G. Cao, "Attack-Resilient Time Synchronization for Wireless Sensor Networks," *Elsevier Journal of Ad Hoc Networks Special Issue on Security in Ad hoc and Sensor Networks*, 5(1), 2007, pp. 112-125.

[9] W. Du, J. Deng, Y.-S Han, P. Varshney, J. Katz, and A. Khalili, "A Pairwise Key Pre-distribution Scheme for Wireless Sensor Networks," *ACM Transactions on Information and System Security (TISSEC)*, Vol. 8, No. 2, May 2005, pp. 228-258.

[10] W. Du, J. Deng, Y.-S Han, and P. Varshney, "A Key Predistribution Scheme for Sensor Networks Using Deployment Knowledge," *IEEE Transactions on Dependable and Secure Computing*, Vol. 3, No. 2, 2006, pp.
62-77.