A Survey on Wireless Sensor Networks Security

Abhishek Pandey
Indian Institute of Information Technology, Allahabad

R.C. Tripathi
Indian Institute of Information Technology, Allahabad

ABSTRACT
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. Today wireless sensor networks are broadly used in environmental control, surveillance tasks, monitoring, tracking and controlling etc. On the top of all this the wireless sensor networks need very secure communication in wake of they being in open field and being based on broadcasting technology. In this paper we deal with the security of the wireless sensor networks. Staring with a brief overview of the sensor networks, a review is made of and how to provide the security on the wireless sensor networks.

Keywords
Wireless sensor networks, security, attacks, security protocol.

1. INTRODUCTION
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. Being of low cost such sensors are deployed densely throughout the area to monitor specific event. The wireless sensor networks mostly operate in public and uncontrolled area, hence the security is a major challenges in sensor applications. The traditional security mechanisms are authentication, symmetric key encryption & decryption and Public Key Infrastructure (PKI) cryptography [8,13,14]. The major challenge is to deploy the above encryption techniques or their counterparts in a sensor network which is characterized with constrained memory, power supply and processing capability [1].

Today Intrusion Detection Systems (IDS) are widely used as a security solution in a wired network in the form of software/ hardware by which one can detect unwanted services going on the system by way of enhanced/abnormal network activity and identify suspicious patterns that may indicate whether the network/system is under attack? For WSN several schemes were proposed but they have limited features like only concern to attacks on a particular layer. Some others have also proposed a theoretical framework that is not suitable at deployment time [16, 17, 19, 24].

Xbow (developer of Mica mote) & Ambient System (developer of µnode) were first two companies who produced sensor nodes for commercial use [15]. Recently Sun Microsystems have also developed a WSN platform that runs java code "on-the-metal" on their motes known as Sun SPOTs[22]. Following table shows the comparative specification of these three popular motes.

	MICAz	µNODE	Sun SPOT
Processor	8-bit Atmel	16-bit TI MSP430	32- bit ARM7 core
Memory	4KB RAM, 512KB flash	10KB RAM, 1MBit flash	256KB RAM, 2Mb flash
Radio	CC1000	CC1010	CC2420
OS	TinyOS	TinyOS	All
Language	nesC	nesC	Java

Table 1: comparative specification of motes

2. COMMUNICATION PROTOCOLS

Wireless sensor networks use layered architecture like wired network architecture. Characteristics and functions of their each layer is given below.

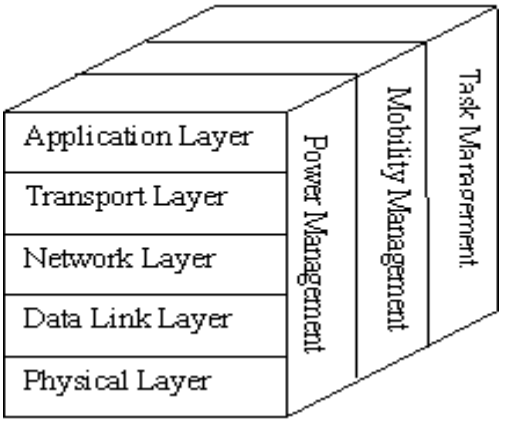

Figure 1 Layered Architecture of WSN

2.1 Physical Layer

The objective of physical layer is to increas the reliability by reducing path loss effect and shadowing. This layer is responsible for established connection, data rate, modulation, data encryption, signal detection, frequency generation and signal detection.

2.2 Data Link Layer

The objective of Data link layer is to insure interoperability amongst communication between nodes to nodes. This layer is responsible for error detection, multiplexing. Prevention of Collision of packets, repeated transmission etc.

To secure data link layer, Karlof et al [2] proposed a link layer security architecture "TinySec" for wireless sensor networks. Naveen Sastry et al[4] proposed Zigbee or the 802.15.4 standard for hardware based symmetric key encryption.

Some researches also proposed the possible use of public key cryptography [3, 9], secure code distribution [10] to create secure key during network deployment and maintenance.

2.3 Network Layer

The objective of Network layer is to find best path for efficient routing mechanism. This layer is responsible for routing the data from node to node, node to sink, node to base station, node to cluster head and vice versa.

The LEACH and PEGASIS are the protocols which describe the techniques to save the energy consumption (power of sensor) so as to improve the life of sensors. LEACH gives cluster based transmission while PEGASIS is chain protocol [5, 6,15].

WSN use ID based protocols and data centric protocols for routing mechanism. In WSN, each node in the network acts as a router (because they use broadcast mechanism), so as to create secure routing protocol. Encryption and decryption techniques are used for secure routing [8,13,14].

2.4 Transport Layer

The objective of Transport Layer is to establish communication for external networks i.e. sensor network connected to the internet. This is most challenging issue in wireless sensor networks.

2.5 Application Layer

The objective of Application Layer is to present final output by ensuring smooth information flow to lower layers. This layer is responsible for data collection, management and processing of the data through the application software for getting reliable results.

SPINS (Security Protocols in sensor Networks)[11] provides data authentication, replay protection, semantic security and low overhead. SPIN has two secure building blocks SNEP and µTESLA. SNEP provides baseline security primitives: Data Confidentiality, two party data authentication and data freshness. µTESLA provides authentication broadcast for severely resource constrained environments.

Localized Encryption and Authentication Protocol (LEAP)[12] is a key management

protocol for sensor networks. It provides multiple keying mechanisms (Group Key, Cluster Key, Pairwise Shared Key) in this regard.

By data Aggregation we can optimize data, network's traffic load etc. Wagner[7] describes resilient aggregation technique for cluster based WSN. Cryptography techniques used by him including the layer wise possible attacks and existing protocols described above are summarized in table2 below.

WSN Layer	**Types of attacks**	**Existing protocols**
Physical Layer	Denial of service attack	
Data Link Layer	Denial of service attack	Link Layer security protocol (TinySec, PEGASIS, LEACH)
Network Layer	Denial of service attack, Wormholes, Sinkholes, Sybil attacks.	Routing protocols (ID based, data-centric)
Transport Layer	Denial of service attack	
Application Layer	Malicious Node	Aggregation scheme

Table2: summery of WSN layers, possible attacks on them and the existing protocols.

3. ATTACKS ON WSN AND THEIR MITIGATION

The security breaches occur primarily in the form of Interruption (breakdown of communication links), Interception (unauthorized access of WSN), Modification (Change of data by unauthorized access) and fabrication (Addition of false data by unauthorized accesses) [13,25,26].

3.1 Denial of service

This type of attack results into making unavailable the resources to their intended users. As an example node 'A' sends request to node 'B' for communication and node 'B' sends acknowledge to node 'A' but 'A' keeps on sending request to 'B' continuously. As a result 'B' is not able to communicate with any other nodes and thus becomes unavailable to all of them.

Denial of service attack may also occur at physical layer by jamming (by broadcasting mechanism) and/or tampering (modification or fabrication) of the packet. In Link Layer it is by producing collision data, exhaustion of resources and unfairness in use of networks. In network layer, it occurs by way of neglecting and the greediness of packets resulting into path failure. In transport layer, DOS attack occurs due to flooding and de-synchronization.

Most of denial of service attacks may be prevented by powerful authentication and identification mechanisms.

3.2 Attack of information in transit

In case of wireless sensor networks usually each node reports changes to a cluster head or base station only for data above some threshold. Information in transit may be altered, spoofed, replayed again or vanished. In this type of attack attacker has high processing power and large communication range. This type of attack may be prevented by data aggregation and authentication techniques.

3.3 Sybil attack

In this attack the attacker gets illegally multiple identities on one node. By this, the attacker mostly affects the routing mechanism.

Sybil attacks are generally prevented by validation techniques.

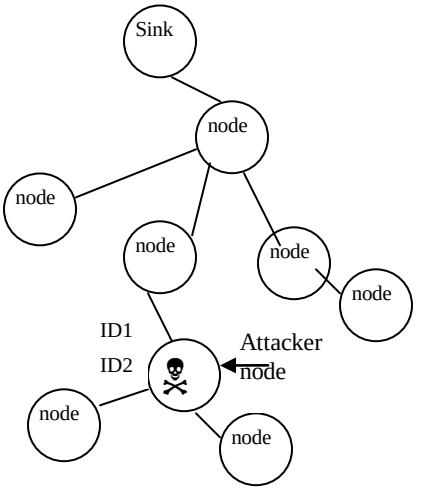

Figure 2: Sybil Attack

3.4 Blackhole/ Sinkhole Attack:

In this type of attack, attacker places himself in a network with high capability resources (high processing power and high band width) by which it always creates shortest path. As a result, all data passes through attacker's node.

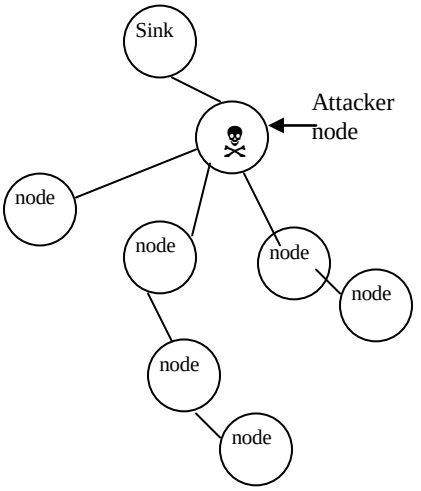

Figure 3: Blackhole/S sinkhole Attack

3.5 'Hello flood' Attack

This is one of the simplest attack in wireless sensor networks in which attacker broadcasts HELLO packets with high transmission power to sender or receiver. The nodes receiving the messages assume that the sender node is nearest to them and sends packets by this node. By this attack congestion occurs in the network. This is a specific type of DOS. Blocking techniques are used to prevent Hello Flood attacks.

3.6 Wormhole Attack

In this type of attack, the attacker uses tunneling mechanism to establish himself between them by confusing the routing protocol.

Figure 4 shows mechanism of wormhole attack let 'Y' wants to send data by way of broadcasting before sending the data to find path. However the attacker '☠' introduces himself as a node 'X' and sends acknowledgement to 'Y'. 'Y' sends data to 'X' that is received by '☠' and '☠' sends that data to 'X' by tunneling, hiding its own identity.

In this case 'X' and 'Y' are not in a single hop but they think they are in a one hop range. The attacker '☠' thus may destroy security by interruption, interception, modification and fabrication.

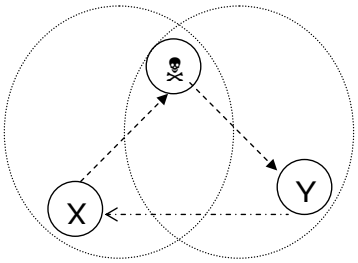

Figure 4: Wormhole Attack

4. SIMULATORS OF WIRELESS SENSOR NETWORKS

For Wireless Sensor Networks there are so many Simulators available. Each simulator has different characteristics and properties. Following are the most commonly used simulators widely used in WSN.

4.1 TOSSIM

The TinyOS provides a TOSSIM as discrete event simulator/emulator. For wireless sensor networks, programs are written in nesC code. For running nesC code in TOSSIM it requires programming interface i.e. written in Python or C++. Python is a powerful debugger which allows dynamic simulation. Transforming code from one to the other is simple in C++. External programs can connect to TOSSIM by TCP socket for monitoring and actuating [21].

4.2 NS2

Network Simulator 2 (NS2) is a most popular discrete event simulator for the Wireless Sensor Networks. It is used it the simulation of TCP, routing and multicast protocol for wired and wireless networks. It supports 802.11 and 802.15.4 type of wireless MAC.

NS2 uses two languages, C++ and OTcl. For the protocol implementation it uses C++, OTcl is used for simulation configuration. Simulation can be observed by Trace file or NAM file.NS-2 does not have good scalability for large sensor networks [18].

4.3 OMNeT++

OMNeT++ is an extensible, modular, component-based C++ simulation library and framework developed in C++. It has simple and powerful GUI library. It is useful for simulation of communication networks, queuing networks and performance evaluation. OMNeT++ is a collection of modules which are written in C++. These modules can be interfaced, nested to form a compound model. The interfacing and nesting is achieved by NED language.

The outputs of the simulation are in the scalar and vector form. For the analysis of the result, we can use simulation IDE[20].

4.4 GloMoSim

Global Mobile Information System Simulator (GloMoSim) is a paraller discrete event based simulator for wireless networks. The simulation is performed by Parsec, a parallel programming language. By this one can simulate upto 10000 nodes. GloMoSim uses layered architecture wherein each layer uses different API these layers are integrated by different API's and may be developed by different people.

Simulators	TOSSIM	NS2	OMNeT++	GloMoSim
Version	Tossim 2.0	NS2.33	OMNeT++4.0	Glomosim 2.0
Architecture	Component based	Object oriented	Component based	discrete event based
Platform	Linux	Linux	Linux, Mac OS and Windows (XP, Windows 2000, Vista)	Linux, Windows
Programming Language	TinyOS	OTCL, C++	C++, NED, GNED	Parsec, C
Standards supported	802.15.4	AODV, OLSR,802.11, Bluetooth, Mobile IP	802.11	CSMA, IEEE 802.11, AOVD, DSR, LAR, TCP, UDP, HTTP, Telnet

Table3: Summary of WSN Simulators

5. CONCLUSION AND FUTURE WORK

This paper gives overview of wireless sensor networks, their security issues and generic solutions. Some applications of wireless Sensor network need a secure communication (like battlefield environment). This paper describes introduction of WSN, Applications, hardware, layered architecture, types of attack its features and countermeasures. The existing security models for wireless sensor networks based on specific network models are also reviewed.

The rapid development in hardware technologies eliminating the hardware constraint like low processing speed, low memory and battery life time of the sensors may soon be overcome/ reduced to enable powerful security measures being adopted in this field.

6. REFERENCES

[1] Jan Steffan, Ludger Fiege, Mariano Cilia Alejandro Buchman,"Scoping in Wireless Sensor Networks", 2nd workshop on middleware for pervasive and Ad-Hoc Computing Toronto, Canada,2004 ACM 1-58113-951-9.

[2] Chris karlof, Naveen Sastry, David Wanger, "TinySec: A Link Layer Security Architecture for Wireless Sensor Networks", Proceedings of the 2nd international conference on Embedded networked sensor systems,November 3-5, 2004, pages 162-172,Baltimore, Maryland, USA. ISBN:1-58113-879-2.

[3] Gunnar Gaubat, Jens-Peter Kaps, Berk Sunar, "Public Key Cryptography in Sensor networks- Revisited", Book Series Lecture Notes in Computer Science Pages 2-18, 11 january 2005.

[4] Naveen Sastry, David Wagner, "Security Consideration for IEEE802.15.4 Networks", WiSE'04, October 1, 2004 Philadelphia, Pennsylvania,USA.

[5] Cauligi S. Raghavendra,"PEGASIS: Power-Efficient Gathering in Sensor Information System", 2002 IEEE Aerospace Conference Proceedings - Volume 3, Big Sky, MT; UNITED STATES; 9-16 Mar. 2002. pp. 3-1125 to 3-1130. 2002 2002.

[6] Siva D. Muruganathan, Daniel C.F. MA, Rolly I. Bhasin, Abraham O. Fapojuwo,"A Centralized Energy- Efficient Routing Protocol for Wireless Sensor Networks", IEEE Communications Magazine. Vol. 43, no. 3, pp. S8-13. Mar. 2005.

[7] David Wagner, university of California "Resilient Aggregation in Sensor Networks", 2nd ACM workshop on Security of ad hoc and sensor networks, Pages 78-87, October 25 2004 Washington DC, USA.

[8] Xiao Chen, Jawad Drissi, "An Efficient Key Management Scheme in Hierarchical Sensor Networks", IEEE MASS 2005 Workshop-WSN05.

[9] Kirk H.M. Wong, Yuan Zheng, Jiannong Cao, Shengwei Wang," A Dynamic User Authentication Scheme for Wireless Sensor Networks", IEE International Conference on Sensor Networks Ubiquitous and Trustworthy Computing (SUTC'06), 2006.

[10] Jing Deng, Richard Han, Shivakant Mishra,"Secure Code Distribution in Dynamically Programmable Wireless Sensor Networks", 5th international conference on Information processing in sensor networks, Pages 292-300, April 19-21, 2006.

[11] Adrian Perrig, Robert Szewczyk, J.D. Tygar, Victor Wen, "SPINS: Security Protocols for Sensor Networks", Department of Electrical Engineering and Computer Sciences, University of California, Berkley, 2002.

[12] Sencun Zhu, Sanjeev Setia, Sushil Jajodia,"LEAP: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks", Aug. 2004, publish in ACM.

[13] Al-Sakib Khan Pathan, hyung-Woo Lee, Choong Seon Hong, "Security in Wireless Sensor Networks: Issues and Challenges", Feb 20-22, 2006 ICACT2006.

[14] Woo Kwon Koo, Hwaseong Lee, Yong Ho kim, Dong Hoon Lee, "Implementation and Analysis of New Lightweight Cryptographic Algorithm Suitable for Wireless Sensor Networks", International Conference on Information Security and Assurance,2008.

[15] Christian Herman and Waltenegus Dargie,"Senceive: A Middleware for a Wireless Sensor Network",22nd international

Conference on Advanced Information Networking and Applications, 2008.

[16] Bo Sun, Lawrence Osborne, Yang Xiao, Sghaier Guizani, "Intrusion Detection Techniques In Mobile Ad hoc and Wireless Sensor Networks", IEEE Wireless Communications October2007.

[17] Zhenwei Yu, Jeffrey J.P. Tsai "A Framework of Machine Learning Based Intrusion Detection for Wireless Sensor Networks", 2008 IEEE.

[18] Tutorial of NS2 http://www.isi.edu/nsnam/ns/tutorial/

[19] Online tutorials http://en.wikipedia.org/wiki

[20] Tutorial of OMNeT++ http://personal.stevens.edu/~hli5/TutorialofOMNET.htm

[21] Philip Levis, "TinyOS Programming ", june 28 ,2006

[22] http://mobilab.wustl.edu/projects/agilla/

[23] Min Chen, Taekyoung Kwon, Yong Yuan and Victor C.M. Leung, "Mobile Agent Based Wireless Sensor Networks", Journal of computers, vol. 1, No. 1, APRIL2006.

[24] Yun Zhou," LLK: A Link-Layer Key Establishment Scheme for Wireless Sensor Networks", IEEE Communication Society / WCNC2005.

[25] Mohammad Ilyas and Imad Mahgoub, "Handbook of Sensor Networks: Compact Wireless and Wired Sensing System", CRC Press, London New York Washington, D.C.

[26] Mona Sharifnejad, Mohsen Sharifi, Mansoureh Ghiasabadi and Sareh Beheshti,"A survey on Wireless Sensor Networks Security", 4th International Conference: sciences of Electronic, Technologies of Information and Telecommunications, March 25-29, 2007, TUNISIA.