Journal of Wireless Networking and Communications 2014, 4(1): 1-6
DOI: 10.5923/j.jwnc.20140401.01

Wireless Sensor and Actor Network – Security Analysis

Binodkumar[1], Malathi Balaji[2], R. Dbalaji[3], Ramkumar Lakshminarayanan[1,*]

[1]Higher College of Technology, Muscat
[2]Sri Krishna College of Engg and Technology, Coimbatore
[3]College of Applied Science, Sallah

Abstract Wireless sensor and actor networks (WSANs) refer to a group of sensors and actors linked by wireless medium to perform distributed sensing and actuation tasks. In such a network, sensors gather information about the physical world, while actors take decisions and then perform appropriate actions upon the environment, which allows a user to effectively sense and act at a distance. WSANs are exposed to numerous security threats that can adversely act the success of import applications. Although WSANs share many common grounds with sensor networks, it is difficult to apply existing security technologies due to the fact that WSANs contain actor nodes that are resource-independent and mobile. This paper aims to study the security aspects of these networks. It paper first introduces sensor networks, its architecture and working and then presents security related problems, threats, risks and characteristics and then finally security defence measures. Additionally, the paper gives a brief introduction to proposed protocols for sensor network security applications. It also highlights experimental work necessary to make these applications more reliable and robust in the real world.

Keywords Sensor network, Actor, Security, Attacks, LEAP Protocol

1. Introduction

In this growing wireless communication era, the researches on wireless sensor networks (WSN), which are rapidly mounting popularity, are also becoming mandatory. The widespread availability of miniature wireless sensor devices that can sense their surroundings and wirelessly communicate with the rest of the world is generating tremendous interest in it[12]. But due to the resource constraints, the sensor devices are not responding immediately and need constant monitoring[2]. Then it has been found that the inclusion of actor nodes in the network improves the performance of the WSN, which is called the Wireless Sensor and Actor Network (WSAN). WSAN derived from WSN refers to a group of sensors and actors linked by wireless medium to perform distributed sensing and actuation tasks. In the network, sensors gather informat ion about the physical world, while actors coordinate and make decisions to perform appropriate actions upon the environment, which allows remote, automated interaction with the environment[1]. Today WSAN networks have spanned over a broad range of civilian and military applications relating to monitoring and control, including health care, habitat monitoring, building surveillance, battlefield reconnaissance and perimeter defense[9]. The physical architecture of the WSAN is given in Figure 1.

* Corresponding author:
rajaramcomputers@gmail.com (Ramkumar Lakshminarayanan)
Published online at http://journal.sapub.org/jwnc

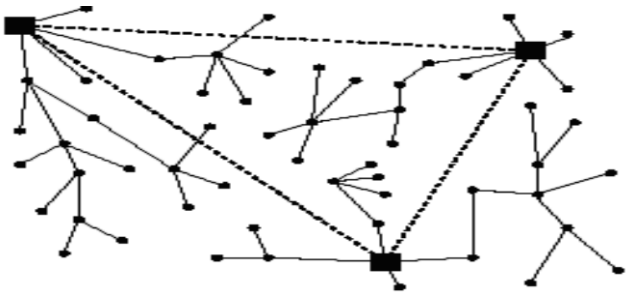

Figure 1.

WSN is a new type of networked system, characterized by severely constrained computational and energy resources, and an ad hoc operational environment. It is a collection of sensor nodes that works collaboratively in multi-hop wireless communication architecture[8]. WSANs share many similarities with sensor networks as they are networks without infrastructure and they use wireless communication technologies. Theyrefer to heterogeneous systems combining tiny sensors and actuators with general-purpose computing elements. These networks consist of hundreds or thousands of self-organizing, low-power, low-cost wireless nodes deployed to monitor and affect the environment as in the figure (2)[3].

Recently WSAN attracted a lot of interest due to the range of applications they enable. The widespread availability of miniature wireless devices that can sense their surroundings and wirelessly communicate with the rest of the world is generating tremendous interest in it. It is giving the vision of anywhere and anytime with pervasive access and computing a reality[4]. A major benefit of these systems is that they

perform in-network processing to reduce large streams of raw data into useful aggregated information.

Figure 2.

Figure 3. Robotic Mule for battlefield

WSANs have large set of applications. They span over a broad range of civilian and military applications relating to monitoring and control, including health care, habitat monitoring, building surveillance, battlefield reconnaissance and perimeter defense[9]. The figures 3, 4 and 5 depict the typical pictures of few WSAN devices. Their emerged applications include habitat monitoring, robotic toys and battlefield monitoring and their emerging applications include location aware in home and offices, biomedical sensing, and of storms, oceans, and weather events monitoring[10].

Figure 4. Robotic Helicopter for enemy spy

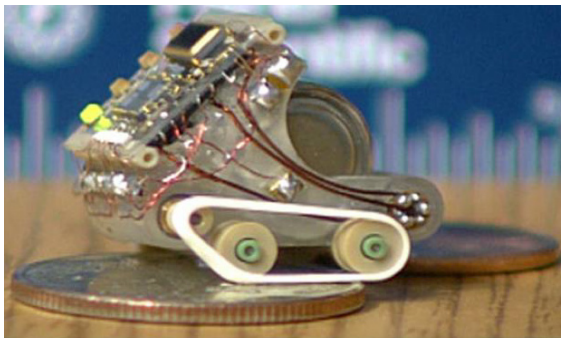

Figure 5. Robot for house monitoring

Unfortunately, WSANs are exposed to numerous security threats that can adversely act on the success of real time implementations. The unreliable communication channel and unattended operation make the security defenses even harder. WSAN system face acute security concerns, including eavesdropping, forgery of sensor data, denial of service attacks, and the physical compromise of sensor nodes deployed into enemy territory[10]. Hence security is a significant concern for many sensor network applications[7], especially the sensor networks those are deployed in battlefield monitoring and home sentry. Fortunately, the new problems also inspire new research and represent an opportunity to properly address sensor and actor network security from the start.

This paper is organized as following. It first introduces the WSANs, their architecture and working and then presents their related security problems, threats, risks and characteristics. Additionally, the paper gives a brief introduction to proposed protocols for WSAN security applications.

2. WSAN Architecture

Recent development of multi-robots and wireless sensor network technologies have lead to the emergence of distributed wireless sensor and actor networks. This kind of hybrid networks not only can observe the environment, process the event data, make decisions based on special event and also, it can perform appropriate actions to interact with the environment[15].

In order to provide effective sensing and acting, coordination mechanisms are required among sensors and actors. Many researches are being carried out to achieve better coordination among them. Moreover, to perform right and timely actions, sensor data must be valid at the time of acting.

WSAN has one or more points of centralized control called base stations also referred to as sinks. (Figure 6). A base station is typically a gateway to another network, a powerful data processing or storage center, or an access point for human interface. Base stations are many orders of magnitude more powerful than sensor nodes. These have enough battery power to surpass the lifetime of all sensor nodes, sufficient memory to store cryptographic keys,

stronger processors, and means for communicating with outside networks. In order to provide effective sensing and acting, a distributed local coordination mechanism is used among sensors and actors.

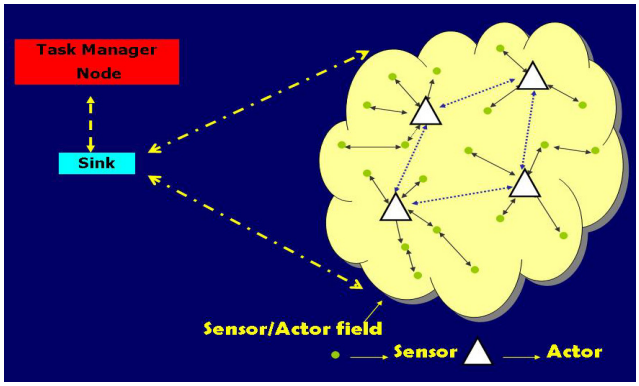

Figure 6. (WSAN Architecture)

WSAN Working

The realization of wireless sensor and actor networks (WSANs) needs to satisfy the requirements introduced by the coexistence of sensors and actors.Sensors gather information about the physical world, while actors take decisions and then perform appropriate actions upon the environment, which allows a user to effectively sense and act at a distance. Base stations control information into the network or extract data from it. The sensor nodes establish a routing forest, with a base station at the root of every tree.

Sensor nodes communicate using RF bandwidth. Each bit transmitted consumes about as much power as executing 800–1000 instructions. The communication patterns within the network fall into the following categories:

- Actor to base station communication, e.g. sensor readings, specific alerts.
- Base station to actor communication, e.g. specific requests, key updations.
- Base station to all nodes (both sensors and actors), e.g. routing beacons, queries or reprogramming of the entire network.
- Communication amongst a defined cluster of nodes (a node and all its neighbors).

3. WSAN Security Issues

Wireless communications are difficult to protect; they are by nature a broadcast medium. In a broadcast medium, adversaries can easily eavesdrop on, intercept, inject, and alter transmitted data, which are shown in the Figures 7, 8 & 9. In addition, adversaries are not restricted to using sensor network hardware. They can interact with the network from a distance by using expensive radio transceivers and powerful workstations. Sensor and Actor networks are vulnerable to resource consumption attacks. Adversaries can repeatedly send packets to drain the nodes' batteries and waste network bandwidth. Since sensor networks will be deployed in a variety of physically insecure environments, adversary can steal nodes, recover their cryptographic material, and pose as authorized nodes in the network. All these lead to a very demanding environment to provide security.

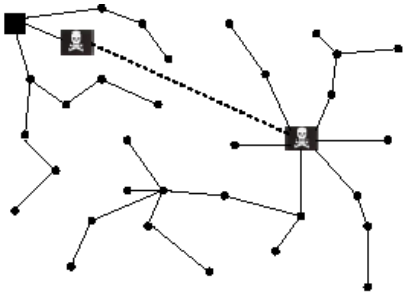

Figure 7.

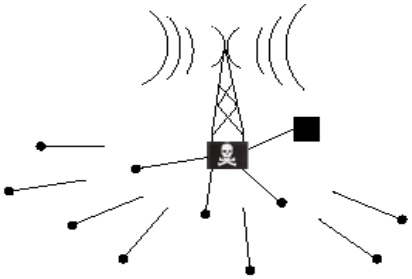

Figure 8.

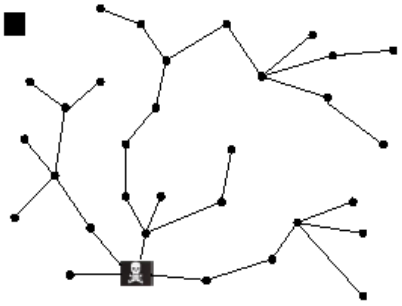

Figure 9.

WSANs share many similarities with sensor networks asthey are networks without infrastructure and they use wireless communication technologies. Unlike traditional sensor networks whose nodes share the same authority and power, actor-based WSANs require a different approach in implementing these technologies. Especially, WSN only consists of sensor nodes which are resourced ependent. And the network structure of WSNs is very simple. Considering both the resource limitation of sensor nodes andthe structural simplicity of WSNs, most key management protocols have been researched by symmetric encryption approach. But WSANs have not only sensor nodes but also actor nodes which are resource independent. Thus, the structural feature of WSANs has to be considered[2].

The 802.11 standard for wireless networks includes a Wired Equivalent Privacy (WEP) protocol, used to protect link-layer communications from eavesdropping and other attacks. But several serious security flaws have discovered in this protocol, stemming from mis-application of cryptographic primitives. The flaws lead to a number of practical attacks that demonstrate that WEP fails to achieve

its security goals[8].

LEAP is also a very popular security solution in Wireless Sensor Networks and it was proposed by Zhu et al in 2004. The Localized Encryption and Authentication Protocol (LEAP) is a key management protocol used to provide security and support to sensor networks. It uses μTESLA to provide Base station broadcast authentication and a one-way-hash-key to authenticate source packets[5]. This protocol is inspired by the idea that every message broadcasted between sensor-nodes is different from another and comprise of different security requirements. In order to meet the variety of security requirements when exchanging messages, having a single key mechanism is impractical, thus LEAP proposes four types of keys assigned to every individual node. The four types of keys established are: individual keys, pair-wise keys, cluster keys and group keys[6]. When we consider the Actor nodes, they are more powerful than the sensor nodes and they may need asymmetric key distribution mechanism. But the LEAP protocol is a symmetric key mechanism and it cannot be used as it is for the WSAN security.

Dai et al. recently proposed a new key pre-distribution scheme based on Rooted-Tree in WSAN[11]. The key management tree is constructed where sink is the root, actors are the branches and sensors are the leaves, to achieve the distributed and integrated key management. One drawback of this key management approach is that some wireless links maynot be keyed and thus a node may need to use a multi-hop pathto communicate with one of its neighbor nodes. Since each sensor node should generate and then store many keys to share with all its neighbors immediately after deployed, the communication and storage cost are generally huge.

A new efficient key management protocol is proposed by YunhoLee, Soojin Lee for the security of WSAN.[2] The application of security is done inlayers or hierarchical method. The upper layer which has less resource limitation with sink and actor is proposed to use security scheme basedon the Public Key algorithm, while lower layer with high resource limitation (sensors) uses scheme based on the Symmetric Keyalgorithm – namely pair-wise, node, and region keys. This protocol can protect the WSAN from many network attacks, but it has to be thoroughly analysed for its effectiveness in real time.

Hence, the other proposed security protocols for WSN including SPINS, LEAP, TINYSEC, ZIGBEE, 802.15.4, MINISEC, LiSP, LLSP and LEDS are also not well suited for the WSAN due to inclusion of smart actor nodes[13,14]. But with necessary refinements, they can be applied to protect the WSAN in a better way.

4. WSAN Research Scope and Challenges

There are three different research areas on WSAN: sensing, communication, and computing (including hard ware, software, and algorithms). Challenges that are faced in the above said areas are Sensor-actor coordination, Coordination among actors, Transport layer, Routing layer, Medium access control, Products development and protection i.e. security[16].

Protecting wireless sensor and actor networks in all is critical. Because they pose unique challenges, traditional security techniques cannot be applied directly to them. Causes are following; first, to make sensor networks economically viable, sensor devices are limited in their energy, computation, and communication capabilities. Second, unlike traditional networks, sensor nodes are often deployed in accessible areas, presenting the added risk of physical attack[17]. And third, sensor networks interact closely with their physical environments and with people, posing new security problems.

Consequently, existing security mechanisms are inadequate, and new ideas are needed. A wireless sensor networks presents significant challenges in designing security schemes. Some of the most pronounced challenges are described below.

4.1. Wireless Medium

The wireless medium is inherently less secure because its broadcast nature makes eavesdropping simple. Any transmission can easily be intercepted, altered, or replayed by an adversary. The wireless medium allows an attacker to easily intercept valid packets and easily inject malicious ones.

4.2. Ad-Hoc Deployment

The network topology always changes due to node failure, addition, or mobility. Nodes may be deployed by air drop, so nothing is known of the topology prior to deployment. Security schemes must be able to operate within this dynamic environment. The ever-changing nature of sensor networks requires more robust designs for security techniques to cope with such dynamics.

4.3. Hostile Environment

The highly hostile environment represents a serious challenge for security researchers. Motes face the possibility of destruction or (perhaps worse) capture by attackers. Attackers may capture a node, physically disassemble it, and extract from it valuable information (e.g. cryptographic keys).

4.4. Resource Limitation

The extreme resource limitations of sensor devices pose considerable challenges to resource-hungry security mechanisms. The hardware constraints necessitate extremely efficient security algorithms in terms of bandwidth, computational complexity, and memory. Energy is the most precious resource for sensor networks; previous work has given little to no attention to energy efficiency. Communication is especially expensive in terms of power.

Each transmitted bit consumes as much power as executing 800-1000 instructions. So security mechanisms must give special effort to be communication efficient in order to be energy efficient.

4.5. Big Scale Network

The high scale of sensor networks poses a significant challenge for security mechanisms. Simply networking tens to hundreds of thousands of nodes has proven to be a substantial task. Providing security over such a network is equally challenging. Security mechanisms must be scalable to very large networks while maintaining high computation and communication efficiency.

5. Security Threats, Types of Attacks and Countermeasures

5.1. Passive Information Gathering

An intruder with a powerful receiver and well-designed antenna can easily pick off the data stream. It allows an attacker to locate the nodes and destroy them. *To minimize the threats of passive information gathering, strong encryption techniques needs to be used.*

5.2. Subversion of a Node

A particular sensor might be captured, and its stored information might be obtained.

Defines an efficient way to disable the node and flash its stored information.

5.3. False Node & Malicious Data (*sleep deprivation torture*)

Intruder can add a node to the system to feed false data or prevents the passage of true data. These messages consume the scarce energy resources of the nodes. Malicious code insertion is one of the most dangerous attacks that can occur. It spread to all nodes and destroy the whole network. The seized sensor sends observations to malicious user. By spoofing, altering, or replaying routing information, adversaries can create routing loops, attract or repel network traffic, extend or shorten source routes, generate false error messages, partition the network, increase end-to-end latency, etc.

Strong authentication techniques can prevent an adversary from impersonating as a valid node in the sensor network.

5.4. Sybil Attack

In a Sybil attack, a node presents multiple identities for other nodes in the network. They pose a significant threat to geographic routing protocols, where location aware routing requires nodes to exchange coordinate information with their neighbors to efficiently route geographically addressed packets. Authentication and encryption techniques can prevent an outsider to launch a Sybil attack on the sensor network.

Public key cryptography can prevent such an insider attack, but it is too expensive to be used in the resource constrained sensor networks. One solution is to have every node share a unique symmetric key with a trusted base station.

5.5. Sinkhole Attacks

In this attack, an adversary lures nearly all the traffic from a particular area (several hops away from the compromised node) through a compromised node, creating a metaphorical sinkhole with the adversary at the center. The adversary spoof or replay an advertisement for an extremely high quality route to a base station. Due to the real or imagined high quality route through the compromised node, it is likely each neighboring node of the adversary will forward packets destined for a base station through the adversary, and also propagate the attractiveness of the route to its neighbors.

5.6. Wormhole Attacks

In wormhole attack, an adversary tunnels messages received in one part of the network replays them in a different part. An adversary situated close to a base station may be able to completely disrupt routing by creating a well-placed wormhole. This creates sinkhole: since the adversary on the other side of the wormhole can artificially provide a high quality route to the base station, potentially all traffic in the surrounding area will be drawn through her if alternate routes are significantly less attractive.

6. Conclusions and Future Work

Wireless sensor and actor networks are major components of the wireless communication. They include resource constrained sensors and smart actors which are connected to the sink nodes. Though they are similar to WSNs in many aspects they differ in their structure and performance. They face a lot of security threats like that of WSNs and all those threats cannot be overcome with the same protocols and mechanisms of WSNs, because of the inclusion of the actors which are rich in resource capabilities. In this paper, few threats and their countermeasures, research scope in WSAN security and few security issues and protocols are discussed. The future work may include the implementation of suitable security mechanisms for the better performance and the outcome of the WSANs in all their applications.

REFERENCES

[1] Zhicheng Dai, Zhi Li, Bingwen Wang and Qiang Tang, 2009. "An Energy-Aware Cluster-Based Routing Protocol for Wireless Sensor and Actor Network." *Information Technology Journal, 8: 1044-1048.*

[2] YunhoLee, Soojin Lee," A New Efficient Key Management

Protocol for Wireless Sensor and Actor Networks", *(IJCSIS) Vol. 6, No. 2, 2009.*

[3] Mayank Saraogi, Security In Wireless Sensor Networks, Department of Computer Science University of Tennessee, Knoxville saraogi AT.

[4] Guest Editorial Security in Wireless Ad Hoc Networks, IEEE Journal On Selected Areas In Communications, Vol. 24, No. 2, February 2006.

[5] Zhu, S., Setia, S., Jajodia S., LEAP: Efficient Security Mechanisms for Large-Scale DistributedSensor Networks. In The Proceedings of the 10th ACM conference on Computer andcommunications security, 2003.

[6] Jang, J., Kwon, T., &Jooseok, S. (2007). A time-based key management protocol for wirelesssensor networks. E. Dawson and D.S. Wong (Eds.): ISPEC 2007, LNCS 4464, pp. 314–328,2007.,

[7] Piya Techateerawat, Andrew Jennings, Energy Efficiency of Intrusion Detection Systems in Wireless Sensor Networks, Proceedings of the 2006 IEEE/WIC/ACM International Conference on Web Intelligence and Intelligent Agent Technology (WI-IAT 2006 Workshops)(WI-IATW'06).

[8] Nikita Borisov , Ian Goldberg, David Wagner, Intercepting mobile communications: the insecurity of 802.11, Proceedings of the 7th annual international conference on Mobile computing and networking, p.180-189, July 2001.

[9] S. Avancha, J. Undercoffer, A. Joshi and J. Pinkston, "Secure Sensor Networks for Perimeter Protection", Computer Networks, Vol. 43, No. 4, 421-435, November 2003.

[10] Jing Deng, Richard Han, and Shivakant Mishra, Enhancing Base Station Security in Wireless Sensor Networks, Technical Report CU-CS-951-03, April 2003.

[11] W. Yu, H. He, and N. Zhang, "RTKPS: A Key Pre-distribution SchemeBased on Rooted-Tree in Wireless Sensor and Actor Network", ISNN2009, PartIII, LNCS 5553, pp. 890-898, 2009.

[12] Wireless sensor network. http://en.wikipedia.org/wiki/Wireless_Sensor_Networks.

[13] Ritu Sharma, YogeshChaba, Yudhvir Singh, "Analysis of Security Protocols in WirelessSensor Network", Int. J. Advanced Networking and Applications 707, Volume: 02, Issue: 03, Pages: 707-713 (2010).

[14] Abu Shohel Ahmed, "An Evaluation of Security Protocols on Wireless Sensor Network" TKK T-110.5190 Seminar on Internetworking 2009.

[15] I. F. Akyildiz, Wireless Sensor And Actor, Networks, School of Electrical and Computer Engineering, Georgia Institute of Technology.

[16] Dung Van Dinh, Minh Duong Vuong, Hung Phu Nguyen, Hoa Xuan Nguyen, Wireless Sensor Actor Networks And Routing Performance Analysis.

[17] Adrian Perrig, John Stankovic,David Wagner, Security in wireless sensor networks,Year 2004 Paper 1217, Communications of the ACM June 2004/Vol. 47, No. 6.