International Journal of Recent Research and Review, Vol. VII, Issue 2, June 2014

ISSN 2277 – 8322

SECURITY ISSUES IN WIRELESS SENSOR NETWORK

Sunita Gupta[1], K.C.Roy[2], Sakar Gupta[3]

[1] *CSE Deptt., JECRC University, Jaipur.*

[2]*ECE Deptt., Poornima University, Jaipur.*

[3] *ECE Deptt., Kautilya Institute of Technology, Jaipur.*

E-mail: gupta_1982sunita@yahoo.com

***Abstract*- A wireless sensor network (WSN) is a wireless network consisting of spatially distributed autonomous devices using sensors to cooperatively monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants, at different locations. A critical aspect of applications with wireless sensor networks is network lifetime. Power-constrained wireless sensor networks are usable as long as they can communicate sensed data to a processing node. Sensing and communications consume energy, therefore judicious power management and sensor scheduling can effectively extend network lifetime. To cover a set of targets with known locations when ground access in the remote area is prohibited, one solution is to deploy the sensors remotely, from an aircraft. The lack of precise sensor placement is compensated by a large sensor population deployed in the drop zone, that would improve the probability of target coverage. The data collected from the sensors is sent to a central node (e.g.cluster head) for processing.**

The security models & protocols used in wired and other networks are not suited to WSNs because of their severe resource constrictions. This paper studies the security aspects of these networks. The paper first introduces sensor networks, and then presents its related security problems, threats, risks and characteristics, Sensor Network System used for Intrusion Detection and for Pipeline Security.

***Keywords:*-Wireless sensor network, coverage and connectivity, security.**

I. INTRODUCTION

The main challenges in WSN are coverage, connectivity and network lifetime. Along with this security in WSN is also an important challenge. In case of sensor networks, it is essential for each sensor node and base station to have the ability to verify that the data received was really send by a trusted sender and not by an adversary that tricked legitimate nodes into accepting false data. If such a case happens and false data are supplied into the network, then the behavior of the network could not be predicted and most of times expected outcome will not be obtained. Sensor networks refer to a heterogeneous system combining tiny sensors and actuators with general-purpose computing elements.

Thus, the resource-starved nature of sensor networks poses great challenges for security. However, in many applications the security aspects are as important as performance and low energy consumption [1]. Besides the battlefield applications, security is critical in premise security and surveillance, building monitoring, burglar alarms, and in sensors in critical systems such as airports, hospitals. A Link Layer Security Architecture for Wireless Sensor Networks is also given in [2]. Basically there are two security system used for security. First is TEDAS Sensor Network System used for Intrusion Detection and second is BODAS used for security in Wireless Sensor Network for Pipeline Security.

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 [4,5], target tracking in battlefields [6], disaster relief networks, early fire detection in forests, and environmental monitoring. Sensor networks are typically characterized by limited power supplies, low bandwidth, small memory sizes and limited energy. This leads to a very demanding environment to provide security. Public-key cryptography is too expensive to be usable, and even fast symmetric-key ciphers must be used sparingly. Communication bandwidth is extremely dear: each bit transmitted consumes about as much power as executing 800–1000 instructions [7], and as a consequence, any message expansion caused by security mechanisms comes at significant cost. In [8], the authors point out that it seems unlikely that Moore's law will help in the foreseeable future. Because one of the most important factors determining the value of a sensor network comes from how many sensors can be deployed, it seems likely there will be strong pressure to develop ever-cheaper sensor nodes. In other words, we expect that users will want to ride the Moore's law curve down towards ever-cheaper systems at a fixed performance point, rather than holding price constant and improving performance over time.

II. SECURITY ISSUES AND GOALS

Sensor networks are used in a number of domains that handle sensitive information. Due to this, there are many considerations that should be investigated and are related with protecting sensitive information traveling between nodes (which are either sensor nodes or the base station) from been disclosure to unauthorized third parties Analyzes the security requirements that constitute fundamental objectives based on which every sensor application should adhere in order to guarantee an appropriate level of security.

III. CONFIDENTIALITY

Confidentiality requirement is needed to ensure that sensitive information is well protected and not revealed to unauthorized third parties. Confidentiality means keeping information secret from unauthorized parties. A sensor network should not leak sensor readings to neighboring networks. In many applications (e.g. key distribution) nodes communicate highly sensitive data. The standard approach for keeping sensitive data secret is to encrypt the data with a secret key that only intended receivers possess, hence achieving. Since public-key cryptography is too expensive to be used in the resource constrained sensor networks, most of the proposed protocols use symmetric key encryption methods.

IV.AUTHENTICATION

The receiver needs to make sure that the data used in any decision-making process originates from the correct source. Data authentication prevents unauthorized third parties from participating in the network and legitimate nodes should be able to detect messages from unauthorized nodes and reject them. Authentication objective is essential to be achieved when clustering of nodes is performed. Clustering involves grouping nodes based on some attribute such as their location, sensing data etc and that each cluster usually has a cluster head that is the node that joins its cluster with the rest of the sensor network (meaning that the communication among different clusters is performed through the cluster heads).

V. INTEGRITY

Data integrity ensures the receiver that the received data is not altered in transit by an adversary. Note that Data Authentication can provide Data Integrity also. Integrity controls must be implemented to ensure that information will not be altered in any unexpected way. Many sensor applications such as pollution and healthcare monitoring rely on the integrity of the information to function with accurate outcomes; it is unacceptable to measure the magnitude of the pollution caused by chemicals waste and find out later on that the information provided was improperly altered by the factory that was located near by the monitored lake.

VI. FRESHNESS

One of the many attacks launched against sensor networks is the message replay attack where an adversary may capture messages exchanged between nodes and replay them later to cause confusion to the network. Data freshness objective ensures that messages are fresh, meaning that they obey in a message ordering and have not been reused. To achieve freshness, network protocols must be designed in a way to identify duplicate packets and discard them preventing potential mix-up.

VII. TEDAS

TEDAS:-Sensor Network System for Intrusion Detection. TEDAS is a wireless sensor network system designed to detect intrusion through the fence around a facility. TEDAS can be adapted to all types of fences, including chain link, wire mesh and iron guardrails. TEDAS identifies unauthorized persons attempting to penetrate a perimeter fence system by force or without permission. The system identifies and locates all unauthorized entry through a fence by cutting the fence and passing through, climbing the fence and jumping over or lifting the fence and crawling underneath. It reduces the probability of false alarms by eliminating natural events, such as wind or heavy rain, and innocuous activities, such as a person leaning against the fence or hitting it with a ball. Sense Node communicate with each other to transmit alarm information over their wireless and/or wired network to the TEDAS Security Center or to other user interfaces as required, such as a mobile phone. The system can be integrated with other devices such as a camera, siren or lighting. Main features of TEDAS are :

- It is Next generation wireless sensor network technology
- High reliability
- Effective monitoring
- `Easy installation
- Cost-effective infrastructure
- Integration with camera, siren or lighting
- Locates incidents with +/-5 m. accuracy
- Command and control software (SenMot)
- Operability with alternative energy sources (such as solar energy)

Fig.1 TEDAS Sensor Network System for Intrusion Detection

VIII.BODAS

BODAS wireless sensor network system for pipeline security is used to detect and localize threats against the safety and security of pipelines through use of line-nodes deployed every 100m along the pipe. BODAS wireless sensor network system for pipeline security nodes constitute a wireless network along the pipeline and pre-process signals from geophones buried between 0.3m and 1m below the ground.

BODAS wireless sensor network system for pipeline security can subsequently localize an intrusion to within 20m of accuracy, and identify a pedestrian within a 30m radius of the pipeline, a person who is digging within a 45m radius, and a truck moving within a 60m vicinity of the pipeline.

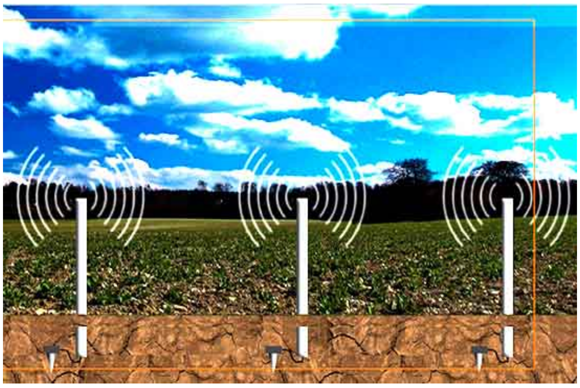

Fig.2 BODAS - Wireless Sensor Network System for Pipeline Security

IX. SPINS

Security Protocols for Sensor Networks SPINS [9] a suite of security building blocks proposed by Perig et. al. It is optimized for resource constrained environments and wireless communication. SPINS has two secure building blocks: SNEP and μTESLA. SNEP provides data confidentiality, two-party data authentication, and data freshness. μTESLA provides authenticated broadcast for severely resource-constrained environments. All cryptographic primitives (i.e. encryption, message authentication code (MAC), hash, random number generator) are constructed out of a single block cipher for code reuse. This, along with the symmetric cryptographic primitives used reduces the overhead on the resource constrained sensor network. In a broadcast medium such as a sensor network, data authentication through a symmetric mechanism cannot be applied as all the receivers know the key. μTESLA constructs authenticated broadcast from symmetric primitives, but introduces asymmetry with delayed key disclosure and one-way function key chains.

IX.CONCLUSIONS

In case of Wireless Sensor Networks, we analyzed the security requirements that should be met to better protect sensor networks from adversaries; confidentiality, authentication, integrity, freshness, secure management, availability and quality of service. As we may see, the same security objectives that exist in conventional systems are needed for sensor networks as well. The difference is that the security objectives here are addressed in the context of sensor nodes characteristics their like their architecture and limitations. We have compared two security approaches TEDAS and BODAS here. Adding security in a resource constrained wireless sensor network with minimum overhead provides significant challenges and is an ongoing area of research.

X. REFERENCES

[1] Sasha Slijepcevic, Miodrag Potkonjak, Vlasios Tsiatsis, Scott Zimbeck, Mani B.Srivastava. On Communication Security in\ Wireless Ad-Hoc Sensor Networks. In The Proceedings of the Eleventh IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE'02), 2002.

[2] Chris Karlof, Naveen Sastry, David Wagner. Tiny Sec: A Link Layer Security Architecture for Wireless Sensor Networks. ACM SenSys 2004, November 3-5, 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] 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.*

[5] 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.*

[6] G.L. Duckworth, D.C. Gilbert, and J.E. Barger. Acoustic counter-sniper system. *In SPIE International* 12 *Symposium on Enabling Technologiesfor Law Enforcement and Security,1996.*

[7] J. Hill, R. Szewczyk, A. Woo, S.Hollar, D. Culler and K. Pister. System architecture directions for networked sensors. *In Proceedings of ACM ASPLOS IX, November 2000.*

[8] Chris Karlof David Wagner. In Secure Routing in Wireless Sensor Networks:Attacks and Countermeasures.

[9] Adrian Perrig, Robert Szewczyk, Victor Wen, David Culler, J. D. Tygar. SPINS:Security Protocols for Sensor Networks. *In The Seventh Annual InternationalConference on Mobile Computing and Networking (MobiCom 2001), 2001.*